DOCUMENT RESUME

ED 363 219 HE 026 829

TITLE	Challenges and Opportunities of Information Technology in the 90s. Track IV: Policy and Standards.
INSTITUTION	CAUSE, Boulder, Colo.
PUB DATE	91
NOTE	73p.; In: Challenges and Opportunities of Information Technology in the 90s. Proceedings of the CAUSE National Conference (Miami Beach, FL, November 27-30, 1990); see HE 026 825.
AVAILABLE FROM	CAUSE Exchange Library, 737 Twenty-Ninth Street, Boulder, CO 80303 (individual papers available to CAUSE members at cost of reproduction).
PUB TYPE	Speeches/Conference Papers (150)
EDRS PRICE	MF01/PC03 Plus Postage.
DESCRIPTORS	Case Studies; *College Administration; Computer Networks; Documentation; Higher Education; Identification; *Information Management; *Information Technology; Management Information Systems; Models; Technological Advancement
IDENTIFIERS	CAUSE National Conference; Computer Security; Data Administration; Integrated Databases; University of Rochester NY

ABSTRACT

Seven papers from the 1990 CAUSE conference's Track IV, Policy and Standards are presented. Topics addressed in this track include data administration, computing access, involvement of constituencies in policy making and enforcement, and institutional standards for departmental systems. Papers and their authors are as follows: "Evolution of a Computer Security Policy: Process and Outcome" (Len Brush and Cynthia Golden); "Disaster Recovery Planning at the University of Rochester: A Case Study" (Nicolas A. Backscheider); "A Case for Common User Identifiers (CUIs)" (Bernard W. Gleason); "A Working Model for Managing Data Standards and Policies In an Integrated Database Environment" (Peter T. Farago and Jessica Whitmore-First); "Adding Value: The Role of Documentation in Application Development" (Donald E. Heller, Joan Perkins, and Steve Csipke); "Issues in the Development of a Campus Computing and Information Policy" (Timothy J. Foley); "The Right Mix: ATMs and VRUs in the Add/Drop Process" (John J. Springfield). (GLR)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED 363 219

Challenges and Opportunities of Information Technology in the 90s

Proceedings of the 1990 CAUSE National Conference

TRACK IV

POLICY AND STANDARDS

November 27 - 30, 1990
Fontainebleau Hilton Resort and Spa
Miami Beach, Florida

HE 026 829

BEST COPY AVAILABLE

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY

CAUSE

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☐ This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy

CAUSE 90
MIAMI BEACH
NOVEMBER 27-30, 1990

TRACK IV

POLICY AND STANDARDS

Coordinator: Jacqueline Brown, Princeton University

Policies and standards can help us stretch fiscal and personnel resources to meet expanding demands for access to information resources. Topics addressed in this track include data administration, computing access, involvement of constituencies in policy making and enforcement, and institutional standards for departmental systems.

BEST COPY AVAILABLE

Evolution of a Computer Security Policy
Process and Outcome

Len Brush, Director
Cynthia Golden, Associate Director

Administrative Systems
Carnegie Mellon University
Pittsburgh, PA 15213

Prepared for Presentation at
CAUSE90
Miami Beach, Florida
November 28, 1990

Evolution of a Computer and Data Security Policy --Process and Outcome

Background	
A Security Policy:	**Who Needs It?**
A Security Policy:	**Who Creates It?**
The Policy:	**What is It?**
The Policy:	**What Happens to It?**
Epilogue:	**Now What?**
Appendix A:	**Summary of the Carnegie Mellon Security Policy**

BACKGROUND

Twenty years ago, as a professor on the University of Michigan Law School faculty, Arthur R. Miller wrote about the uses and abuses of the then somewhat new information technology in his book *The Assault on Privacy--Computers, Data Banks, and Dossiers.* He wrote, "No people in the world are scrutinized, measured, counted, and interrogated by as many poll takers, social science researchers, and governmental officials as are Americans." Professor Miller's book followed closely the debate in 1967 about a proposed National Data Center.

Thirteen years ago, the report of the Privacy Protection Study Commission submitted its final report on "Personal Privacy in an Information Society" to the then President of the United States, Jimmy Carter. The commission was created by the Privacy Act of 1974 and emphasized the public sector during the course of its study and addressed the issues of personal privacy in the public sector as well. From each of these efforts it is not only reasonable, but imperative to conclude that the ever-increasing capabilities of information technology may run counter to a constitutional right to privacy endowed upon each and every American citizen.

The issue of creating countermeasures, i.e. technological security systems, to counteract unwarranted infiltration into more and more technologically sophisticated information handling systems seems at best an endless occupation of time and energy. Indeed, it is an endless pursuit for which patience, diligence, and tenacity provide the only vehicle.

One only has to look at the computer security industry which has sprung-up around the information technology industry in the past twenty years to realize that the threat to personal and proprietary privacy is a real and serious modern sociological phenomenon of the latter part of this century. So, what is going on, anyway? In some real sense, the purveyors of technology in the information handling environment in which most of us are engaged become the first members of our society to recognize the threat to their own "personal privacy." The fear and knowledge of this threat prompts the information technologists to respond positively when the non-technologist (i.e. the social and political scientist, the lawyer, the business manager as well as others from non-technological venues) inquire into the "safeness" or security of both personal and (corporate) proprietary data.

Nowadays when someone asks about "security of data" they usually refer to that information (policies, procedures, programs, and data) that is processed "on a computer." Further, these same inquirers usually are talking about that information which is entered into, processed, stored, and retrieved from the "central computer" or "the corporate data center" or "the mainframe." The important point here is not the terminology but the fact that when the non-information technologist raises the specter of information security or the lack thereof, that person: (a) is really concerned about a potential privacy invasion and (b) has a receptive audience in the person of the technologist.

Computer and data security have, indeed, long been the province of the technologist. Auditors have not been concerned about information privacy, computer security breach, computer virus invasion, or database invasion nearly as long as the computer scientist or information systems professional. This is no longer the case, however. The auditors have discovered a fertile ground for plying their trade and in the process have created perhaps one of the fastest growing career paths for both the traditional auditor as well as the information technology professional.

At Carnegie Mellon University, the need for improved security in and around the data and information systems has been highlighted by a confluence of three separate interests. The first of these is the interest in, responsibility for and authority over the central computing environment through which most of the University's "business" data flows. This interest, responsibility, and authority comes from the view of the technologist, those responsible for the hardware, software, and applications which reside predominantly "in the data center machines."

Almost simultaneously, the University's external auditors began to raise questions about the security or lack thereof of business data, the absence of clear cut university policies and procedures (governing the protection of privacy and security of information), and the vulnerability of the data center to various types of disaster.

At the same time various members of the University's Board of Trustees had, predictably, heard numerous horror stories about the Internet worms, hackers, computer viruses, and last but not least, "Robert T. Morris"[1] . These trustees, mostly "non-technologists," and some CEOs of prominent U.S. firms, began to question the University's degree of readiness to ward off a potential attack on the information resources of the University. These were and are imperative concerns. The information systems technologists who had quietly been creating countermeasures at the operating system, database management system, and application-level finally received support and demand for those efforts (for the first time.) The auditors and the trustees provided the business reason to formalize what the technologists had created but had not yet fully documented into formal policies and procedures.

The effort to create a security policy actually began in 1988 in an attempt to document the requirements for data security which applied to a new family of administrative information systems. About that time, the external auditors submitted their second annual report which cited the University for "the lack of a computer security policy." By this time, most of the Trustees had heard of Robert T. Morris and the internet worm of November, 1987.

The confluence of concerns over information privacy and the security of University business data by the non-technologists (auditors and trustees) and the technologists (information systems professionals) created the impetus to develop the security policy about which this paper reports.

A SECURITY POLICY: WHO NEEDS IT?

Can't we just concentrate on computer security and forget about the policy? This depends somewhat on who are the "we?" As stated earlier, if "we" are the technologists then "we" have been concerned about computer security; "we" have implemented numerous measures to secure the privacy of and proprietary right-of-access to the computer and its store of information. Clearly, the information technologists have implemented security measures usually within the operating systems to either prohibit or at least monitor acts of irresponsibility, probing or hacking and penetration.

---

[1] --In real life, Robert T. Morris, Jr. of Cornell University, Ithaca, NY, alleged perpetrator of the now famous November 2, 1988 Internet worm.

Database security via DBMS software and applications security via a separate layer of software represents still other attempts by the technologists to inhibit and monitor unauthorized acts against the data.

The security policy works as a two-way instrument of communication -- the documentation of the dialogue between the technologist and the non-technologist. The technologist participates in this dialogue by expressing in general terms the technical feasibility of securing the computer against unwarranted infiltration and compromise. The non-technologist can state fears and reservations as well as express management parameters against which security will be assessed. Parameters such as cost, complexity, and control are not uncommon even if not explicitly recited in a security policy.

These parameters, when viewed in the context of technical feasibility, become a medium of exchange between the technologist and non-technologist for arriving at a policy which is enforceable and cost-justifiable. An issue to ponder is that just as the securing of computer systems is neither inexpensive nor without opportunity costs, nor is the creation, selling, implementation, and enforcement of the policy. The policy itself takes time and effort to develop that might otherwise be applied to other initiatives.

Who needs it? Certainly the technologist needs it. A statement of security policy lends corporate or institutional credence to the security efforts of the technologist of the past 15 to 20 years. Further, the technologist knows that security is not free. Some hardware vendors have labored for years to protect sensitive information from unwarranted access and as a result added to the complexity and cost of the controlling software. Although not true in every case, vendors with proprietary operating systems tend to produce more secure computing environments than the so-called "open systems vendors." This trend is changing, however, with assistance of the federal government. In fact, one challenge for the next 10 years will be to secure "open" systems to the same or greater degree than existing proprietary operating systems.

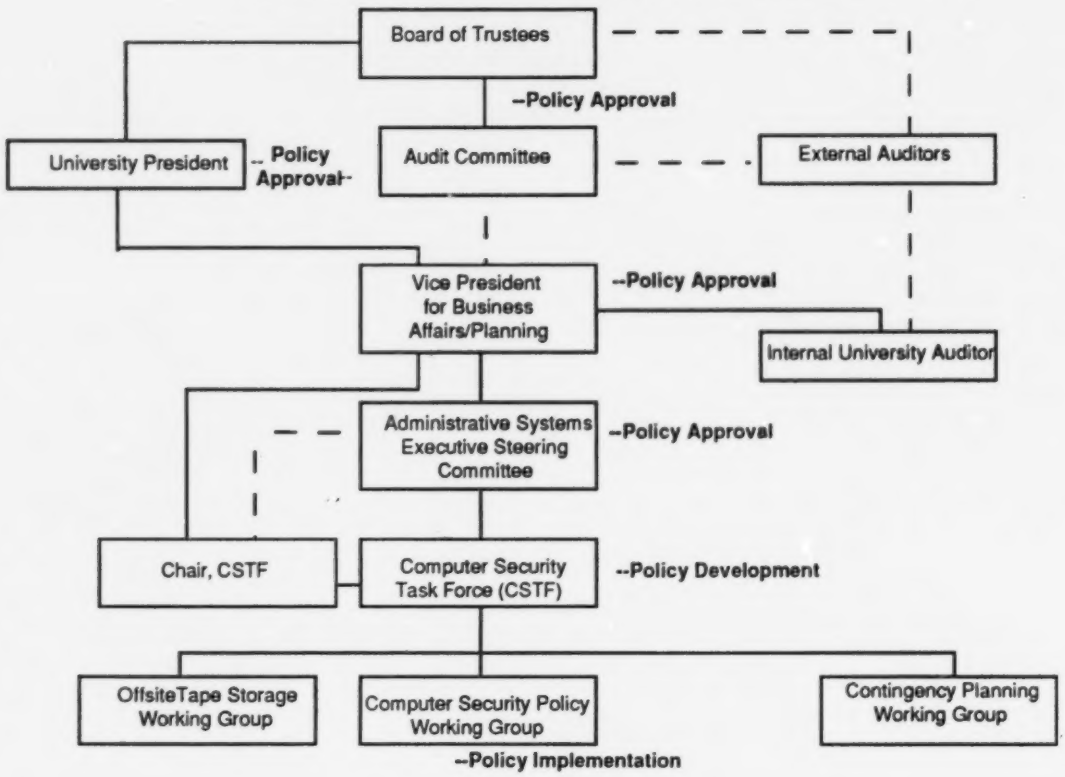
A SECURITY POLICY: WHO CREATES IT?

The genesis of the policy can be found in various comments from the external auditors (Deloitte Touche) as expressed in their management letters to the University over a two to three year period. Further, the trustee Audit Committee assigned the development of a University policy to the Vice President for Planning. Subsequently, a Computer Security Task Force was established to develop a policy covering and governing security of the University's administrative data and its administrative computing systems. The following staff were assigned to the task force:

- Project Director, Student Information Systems (Planning Division)
- Director, Administrative Systems (Planning Division)
- Manager of VMS Software (Academic Services Division)
- Assistant Director, Administrative Systems (Planning Division)
- Associate Director, Administrative Systems (Planning Division)
- Manager of Internal Audit (Business Affairs Division)
- Director of Business Systems (Business Affairs Division)
- Director of Enrollment Systems (Enrollment Division)
- Registrar (Enrollment Division)
- Director of Development Information Systems (Development Division)
- Director of Human Resources (Business Affairs Division)
- Manager, Operations and Special Projects (Academic Services Division)

The intent of the task force was to present an approved policy to the trustees Audit Committee on April 27, 1990. The Computer Security Task Force is also an outgrowth of the previously constituted administrative systems security task force created in 1987 and has been stimulated by the continuing concerns for security as expressed in the auditors' management comments of their past three audits of University operations. The Computer Security Task Force was also charged with development of an off-site Tape Storage Plan and Disaster Recovery (or Computer Contingency Plan). The organization put in place to develop the security policy, as well as these other two charges, is shown in Figure 1.

FIGURE 1. ORGANIZING TO CREATE A SECURITY POLICY



In addition to the organization which evolved to create the computer security policy, many other concerned constituencies were invited to review, critique and offer suggestions to the policy. The notion that any segment of the University was either inadvertently or purposely excluded from the policy development would be unlikely. All formal organizational channels of communication were utilized in an attempt to subject the policy to careful scrutiny. This careful scrutiny was deemed essential inasmuch as the resultant policy would have the full force of the Board of Trustees, the President's Office, and the Dean's Council behind it. Further, the policy carries with it significant authority for disciplinary action in the event of willful violations of the computer or data security rules and regulations. Therefore, the time-consuming review and evaluation of the policy as it evolved was deemed appropriate by the formal organization charged with the policy's development. The constituent groups and individuals who participated in the review and evaluation were:

- The Dean's Council
- The University Faculty Senate Chair
- The President's Staff
- Director of Campus Security
- Affirmative Action Officer
- Dean of Student Affairs
- Business Manager's Council
- Associate Dean's Forum
- Student Representatives to the Board and the Faculty Senate
- Software Technicians

The groups and individuals participated in the review at different points in the process, some participating more than once.

THE POLICY: WHAT IS IT?

The Carnegie Mellon University "Data and Computer Security" policy is a Board-approved document that was developed by the Computer Security Task Force. The policy development took place over 10 months between November, 1989 and September, 1990.

The security policy applies to administrative data on central and distributed computers and currently does not apply to academic or research data. Only employees of the university are permitted access to this data. Access by non-employees is possible only if special permission is granted and a need-to-know is established.

The justifications for the policy are based on the importance of data as a "valued resource over which the university has both right and obligations to manage, secure, protect and control." The need to protect this data and the importance of defining the responsibilities of those who handle the data have prompted the development of this policy document.

The policy itself is divided into two parts, the first addressing security administration and the second outlining security procedures. The following sections briefly describe the contents of the document.

Security Administration

Many units within the university are essential to the development and enforcement of a comprehensive security policy. At Carnegie Mellon, these groups include the Administrative Systems department, the Computing & Communications group, administrators, executives and staff.

As mentioned previously, the Computer Security Task Force is comprised of members of all of these groups, appointed by the President and responsible for the maintenance of a secure administrative data processing environment. The task force formulates overall policy, addresses issues that effect computer security, reviews situations involving violations of policy and provides guidance for implementation and interpretation of policy.

The Administrative Systems department is responsible for the design, programming and maintenance of administrative applications, while Computing & Communications maintains and operates most of the computing equipment on which most of these applications reside. Both groups are responsible for proper security controls.

Fundamental to the policy and the administration of it are three new responsibilities at Carnegie Mellon: the "Data Owner," the "Data Security Officer" and the "University Data Security" officer. The Data Owner is the employee of the university who is responsible for the data in the system. In most cases, this is a division or department head. The responsibilities of the Data Owner include evaluation and approving requests for access to specific data or groups of data and ensuring the accuracy and quality of data residing in application systems.

The Data Security Officer (DSO) is the employee responsible for evaluation and monitoring systems access. He or she will evaluate requests for access to application systems and decide whether to authorize or deny the request. In addition, the DSO is in charge of establishing and deleting computer user-ids, resolving security issues and periodically reviewing the access privileges that have been granted to users. The Data Security Officer typically reports to a Vice President or other Executive level person. The University DSO works with the individual DSOs to provide over-all coordination, and serves as a focal point for university-wide enforcement of the security policy.

Although in practice, these tasks have been performed informally by users and technologists for many years, the policy officially recognizes these functions and clearly spells out, by application, who "owns" the data. The committee determined that it was important to the successful implementation of the policy that the data owner and DSO's responsibilities be explicitly defined.

The development of the concept of the DSO took many months to finalize. Members of the committee were concerned about the number of DSOs that would be needed, if there should be a University DSO and how much additional work would be required. Because administrative computing applications divide into three major functional areas, Enrollment Systems, Business Systems and Alumni/Development Systems, one DSO for each of these application areas evolved. Each DSO will work with many data owners in his or her division. For example, the DSO for enrollment systems applications will work with data owners in her division: the registrar (for student records), the director of admissions (for admissions data) and the director of financial aid (for financial aid data).

The actual responsibilities of the Data Security Officer and how those responsibilities related to those of the data owner were discussed at length during policy development. The model as presented here reflected what was currently being done in some areas, and set very clear paths for granting and monitoring access to data.

In addition to looking at who owned the data and who was responsible for determining how it could be used, it was necessary to examine the data themselves. The committee looked at the kinds of data that were stored in administrative databases and how these data were used. As a result of the examination, all university data were divided into four categories: public information, campus-wide information, restricted information -- moderately sensitive, restricted information -- highly sensitive. Classifying data based on their "accessibility status" made the tasks of identifying data security officers more reasonable. Table 1 delineates the data classes and accessibility guidelines.

TABLE 1. Accessibility of Data by Type

Data Type	Public Information	Campus-Wide Information	Restricted, Moderately Sensitive	Restricted, Highly Sensitive
Employee Data	Government forms requiring salary data; (IRS Form 990)	University Information	Appointment Information Non-salary related benefits enrollment information Biographical Information Employee Information Salary surveys	EEO Information by employee Salary Information by employee Termination / Disability Information by employee
University Finances	Annual Reports	Internal Annual Reports Quarterly Reports	Financial data by operating unit	None
Facilities	None	Building Use Information (Fact Book) Building Floor Plans	Building Maintenance Information	None
Students	*Directory* Information as identified in the university policy on "Privacy Rights of Students"	None	Biographical Information Academic Information	Financial Aid Information Parent's Financial Information Student Accounts Receivable Information Students Payment Information Career Service Information

Alumni and Friends	None	None	Biographical Information	Gift and Pledge Information Financial Information Employment Information Biographical Information for Friends
Education and Instruction	Programs Offered Degrees Offered Courses Scheduled	Faculty Course Evaluation Results	Instructor Information	None
Research Activities	None	None	Proposal Information	None

Procedures

Specific procedures were defined to address the daily administrative computing business as it relates to the new security policy. Defined in the document are minimum security measures that are required for the operating systems, database management systems and networks used by administrative applications. The applications themselves must be examined on a case-by-case basis, so that security requirements can be determined. The often complex interaction with other applications, the operating system, the underlying databases, and the needs of the user community preclude an overall policy for application-level security.

Backup and recovery procedures explicitly require that administrative backup data be stored off-site, and that an approved disaster recovery plan be written and implemented to cover situations in which hardware and/or software cannot run in its normal environment. The DSO is charged with periodically reviewing the procedures that affect his or her area.

Passwords and the management of them is specifically addressed by the policy. Guidelines for password selection will be distributed to all users, specifically noting that sharing of passwords violated the policy. A password monitoring program was written as a result of building this policy, and is run on a regular basis. Users with insecure, easily guessed passwords are notified and required to change their current password.

Procedures to be used in managing systems for employee turnover have also been described in the policy. Automatic notification will be sent to appropriate account managers in the event of an employee's termination. Access to accounts will automatically be suspended, pending final authorization for deletion. This action serves to protect the employee in the event of any problems as well as to protect the university against any possible systems tampering.

Specific procedures that explain how a given employee can gain access to administrative data are spelled out in the policy. These procedures involve completing an application form and securing the approval of the Data Owner. In the event the Data Owner denies access, the decision can be appealed to the Administrative Computing Security Committee, which has the final decision in these cases.

Finally, the policy deals with maintaining confidentially of data, reporting security breaches and enforcing penalties. Administrative information generated by the university's administrative systems must be in compliance with regulatory requirements, (such as the Buckley Amendment) or university policy, (such as salary data are not public information). The Data Owner is responsible for determining what data can be released, to whom and the method and time of of its release.

In the course of performing job duties, many employees have access to restricted information. Their responsibilities to maintain the confidentiality of these data are clearly listed. Unauthorized release of restricted information can result in disciplinary action and possibly dismissal. Review of such cases is the responsibility of the Administrative Computing Security Committee, which will recommend the appropriate action. Referral will be made to the Provost, the Director of Human Resources or the Dean of Student Affairs, where appropriate. Matters involving individuals not affiliated with the university will be reviewed by the university attorney.

THE POLICY: WHAT HAPPENS TO IT?

Once the policy had been written and agreed to by the committee, the next step was to obtain university approval. The policy document went through a series of revisions, based on comments that were solicited from various campus groups. The document was distributed to the Business Managers Council, the Enrollment Management group and the President's Council for comments during various stages of its development. Final approval was given by the Executive Steering Committee before it was present to the audit committee of the board of trustees. The formal policy was issued in June of 1990.

Implementation Plan

Writing a security policy is only the first step -- implementing it is perhaps the more difficult and challenging part of the task. Upon approval of the policy document, a subcommittee of the Security Task Force began the process of putting together a plan that would put the policy into practice. The objectives of this plan are:

1. the identification of responsibilities, actions and resources necessary to insure proper implementation of the policy

2. the assignment of specific responsibilities outlined in the policy to specific individuals

3. the development and implementation of campus-wide training and communications initiatives regarding issues of data and computer security

Detailed tasks lists were produced for the Data Security Officer, and the tools that he will need to perform each task were defined. In order to establish new user-ids and to monitor user behavior, the DSO requires a series of status reports for users and system resources and on-line access to some system utilities. Standard reports that are necessary to the DSO's functions include lists of valid users for a given application, lists of permits for each user, report of terminated employees, 'insecure' passwords, log-in attempts that failed and lists of user-ids with passwords that have not been changed in 90 days. These must be put into production and distributed to DSOs on a regular basis.

The DSO also must work closely with the technologists, particularly those in Administrative Systems who set up access privileges, to ensure that the application systems that are released meet the proper security requirements. Although much of this had been accomplished informally in the past, the approval of the policy clearly defines the official responsibilities and roles of individuals within the university with regards to enforcing a security policy.

A list of individuals to be designated as Data Security Officers was compiled and presented to the Executive Steering Committee for approval. By December 31, 1990 the necessary tools (reports and procedures) needed by the DSOs are scheduled to be in place. The implementation plan including campus communication and training, will begin in December, 1990 as well. A wide variety of media are scheduled to be used to publicize the policy, including organizational announcements, newsletters and electronic bulletin boards. A document summarizing the policy has been mailed to all current users of administrative systems and data. Training for campus users will be conducted on a regular basis. Initial plans call for members of the task force to train key departmental contacts who, in turn, will train departmental users.

Epilogue

Just so we don't get to blinded by the light cast from (development of) the security policy, it must be remembered that the real issues of concern to both technologist and non-technologist are security of information and computer-based resources. The security policy is simply the vehicle to communicate the concern about and interest in information resources to the institution, firm, agency or other organizational entity. The advocated theme of this paper is that the policy communicates the concern, consolidates potentially disparate procedures and provides authorization to enforce security. In the instance of Carnegie Mellon University the security policy is authorized at the highest organizational levels. The Board of Trustees responding to its own fears and the admonishment of the University's external offices directed the President's office to create the policy.

Given the policy, we now must turn our attention to the multiple threats. As stated in the Background section of this paper, concerns emanate from legal issues, from privacy concerns and even national defense. Commerce and industry have responded to multiple threats; so, too, has higher education. The obvious and rapid evolution of computer and communications technologies has placed society into an ever-changing scenario of security measures, countermeasures and counter-countermeasures implementation.

In the late 1960s, the main "security" concern was for the physical security of "the computer". This was, at least, partly due to the enormous capital cast of the then, mainframe hardware. Data security was not the key issue in the sixties. But with the advent of data communications lines into and out of the computer room in the seventies, the threat to corporate and personal data became a key concern. The eighties were the decade of the microcomputer and the needs of the "end-user".

And what about the nineties and beyond? The information society is upon us; computers are in the hands of all organizational personnel. Computers guide the flow of information and the business flow of the firm. So we cannot pat ourselves on the back because we developed a policy. The policy is a good start but only a start. So what is next?

The security policy must continue to have the full force of College and University authority behind it. The implementation of the policy calls for an increased awareness on the parts of many campus constituents, some of whom were not directly involved in the policy development. Who are these constituents? Students, faculty, administrative staff, database administrators, the newly-defined "data owners" and "data security officers," systems programmers, campus security officers, human resource trainees, University Ombudsman, legal staff and many more will need to learn, understand and live with the new security environment.

In addition to education, public information (e.g. the public announcement to the entire campus as shown in Appendix A), and specific training, all persons who handle data will be expected to be accountable for their day-to-day activities in the handling of data.

To supplement the policy, the University is developing a contingency plan for dealing with the many potential threats passed to both central and distributed computing environments on campus. The policy in intended to deal primarily with threats imposed by humans through raising levels of consciousness about the simple accidents as well as potential errors of omission and commission perpetrated by employees and others.

The policy also seeks to guard against unrestricted access and provide authorization for better controls, procedures and management over the domain of institutional data and information. The contingency plan seeks to provide for continuation of business in the event of either a physical disaster or an electronic invasion. Hackers can be a electronic problem, viruses and worms are a problem that exist either through electronic communications or magnetic media or both. The contingency plan also seeks to guard against the stoppage of business due to obvious threats of fire, water, power outage, explosives, glycol leaks and the like. Off-site storage of valuable institutional data is already in place; we could ill-afford to lose the institutions data resource because we kept it in close proximity to the "computer room". Many firms provide excellent, safe storage condition just to protect against loss due to having all the "eggs in one basket".

Security requires a policy but the policy is not a guarantee of security. Information security is a great management challenge and is a little like insurance; it costs money, may even be expensive and it doesn't help you much until you need it.

APPENDIX A

PUBLIC ANNOUNCEMENT TO THE UNIVERSITY COMMUNITY

University Policy Statement

Access to data residing in administrative systems and applications at Carnegie Mellon University is to be granted only to those individuals who must, in the course of exercising their responsibilities, use the specific information. Access to administrative data will be granted to university employes only. Individuals outside the university can be authorized access to university data only if that authorization is granted by an Executive Officer of the university. Access and update capabilities/restrictions will apply to all administrative data, data stored on the Administrative Systems computers and on mini-computer and micro-computers across campus. Security measures apply to administrative systems developed and/or maintained by university departments or outside vendors, and **not** to academic/research computing.

Requesting Authorization for Administrative Data Update or Inquiry Capabilities

1. Fill out requests for access, indicating specific categories of information needed.
2. Have your supervisor approve the request.
3. Send the form to the Data Security Officer for approval.
4. The Data Security Officer will issue you a user id and password, in addition to provide specific information related to the application.
5. If you are denied the capabilities requested, you can appeal that decision to the Administrative Computing Security Committee.

Your Responsibilities as a User of Administrative Data

Use of Your User ID and Password

You are responsible to maintain the security of your user id and password, which permits you access to administrative data. You should use passwords which would not be easily assessed by an unauthorized user. Under no circumstance should you allow another individual to access data under you user id and password. Remember--you are responsible for any activity taking place under your user id and password.

Use of Administrative Computing Resources and Data

Access to administrative data is granted only to those individuals who need to use the specific information in the course of their responsibilities. Computing is a resource, and as such, should be used wisely. As a result, please practice good computing habits by logging in only when needed, trying to consolidate various tasks on the system, etc. This will help to improve the performance of the computing systems for all users, Also, data is to be used for job-related purposes only. Please use discretion in the handling of data.

Maintaining Confidentiality of Restricted Data

In the course of accessing data or information, you might access restricted information within the particular database. The following guidelines apply:

- When accessing restricted information, you are responsible to maintain its confidentiality. The granting of a user id and password assumes that you will maintain confidentiality over appropriate information without exception.
- The release of restricted data without the express approval of university management or outside the guidelines established for such data will not be tolerated.
- Unauthorized release of restricted information will result in appropriate disciplinary action, including possible dismissal.
- If you are aware of possible breaches in administrative data/computer security, you are expected to report such occurrences to the Administrative Computing Security Committee.

University Contacts

Contact	Telephone	E-Mail Address
Manager, Internal Audit	(412)268-2011	ah24 @ andrew
Director, Administrative Systems	(412)268-2835	lb1z @ andrew

Disaster Recovery Planning at the University of Rochester: A Case Study

Nickolas A. Backscheider
University of Rochester
Rochester, New York

Abstract: The University of Rochester had recognized the importance of disaster recovery planning for a long time, but it was not until it became involved in a smaller project, developing a contingency plan for payroll, that serious work on disaster recovery planning began. This case study reviews the history of the situation and draws some conclusions about effective disaster planning.

Disaster Recovery Planning at the University of Rochester: A Case Study

For a long time the University of Rochester recognized that disaster recovery planning was something that it ought to take seriously. It arose at steering committee meetings where the typical comment was "we really ought to consider. . . ." It arose year by year in the reports of the University's auditors. It arose among our computing managers and resulted in sending someone to a three-day conference on disaster recovery planning on an island in Florida. Some of the administrative offices, the registrar in particular, developed contingency plans for use in case the computers were unavailable just before graduation. (The University of Rochester, you see, has a long tradition of actually handing diplomas to graduating students during the ceremony, and that's not a good time to be guessing whether or not someone finished all the requirements.) There was no question that the University recognized disaster recovery planning as a "good thing."

But, all the while we recognized the wisdom in preparing a disaster recovery plan, we also recognized some very apparent drawbacks and difficulties. First, disaster recovery plans cost a pile of money. The little bit of investigation that we had done revealed to us both the expense of preparing the plan and the high cost of such backup facilities as hot sites and cold sites. Second, The preparation of a disaster recovery plan seemed sure to interfere with the daily operations of our staff, not just the computing staff, but the student records staff, the personnel staff, the finance staff, and everyone seemed always stretched too thin to take on another major project. Third, in the back of the minds of senior administrators was the concern, I suspect, that this would be another time when Information Services would ask for more staff. How would you justify that request against the requests and demands of other departments? But finally, the most telling argument was probably the feeling that disasters really happened elsewhere and that a large number of resources were required for the preparation of a disaster recovery plan to protect against something that was probably not going to happen.

The result of these conflicting perceptions of disaster recovery planning--—that it was both beneficial and expensive— was an attempt to do it for free. Well, not exactly for free, but with information services picking up most of the tab out of funds already allocated. After all, the argument ran, planning for computer disasters is the responsibility of the information services group. Under the leadership of the Director of Administrative Information Services, the University engaged a consultant to help us with the planning.

The value we received from this was, in my opinion, mixed. On the one hand we received a good survey of risks that we could control, actions that would lower the probability of disaster. The survey pointed out fire and water hazards, demonstrated that the access control to the computer room was not as tight as it should have been and that there was room for improvement in tape handling and storage procedures. The results of the survey were taken quite seriously by the computing staff and numerous physical and procedural changes were made.

On the other hand, we received a two inch thick notebook that looked like a disaster recovery manual on the outside, but which probably would have been of little help in a disaster. The notebook included a generic outline of a plan, but not enough detail to guide our actions. It included forms for listing vendors, but I don't think that either the list of vendors or the lists of equipment that would be needed in case of a disaster were completed. It specified that the highest priority systems would be restored first, but when departments had been interviewed in an attempt to obtain priorities for recovery, the results were lists of the week by week activities of each department with no differentiation as to importance. Now clearly not all of these lapses are the fault of the consultant, maybe none of them are; we could have been more assiduous in carrying through. But the most dangerous thing about this disaster recovery plan was not that it was generic, or that the procedures were only partially documented. The most dangerous thing was that for several years some of the top managers of the University lived under the impression that not only did we have a disaster recovery plan which protected us, but that we had achieved it for practically no cost either in dollars or in staff time.

The estimated recovery time of this recovery plan was six months for administrative computing at the University. That's a long time for employees to put off the landlord or do without groceries. It's a long time to interrupt the development fund drive. It's a long time to compute grade point averages for 4000 undergraduates by hand, and it's a very long time to run a hospital without a full complement of employees.

To their credit, some of the information systems directors decided to seek a way that would allow them to run critical programs, especially payroll, during a disaster. Still looking for an inexpensive way to do this, they attempted to write an agreement with a nearby school that would, in the event of a disaster, allow either school to use the other's computing facilities for critical jobs. The idea sounds great, and both schools worked hard on it, but eventually it came to naught. The problems centered about issues of cost and control. One problem centered about keeping the two systems congruent. It appeared to be an

expensive proposition to upgrade a system because your partner did. It looked like a very time-consuming business to meet weekly with your partners across the city in order to keep up-to-date on system corrections and changes. And the people in charge began to worry about how such an agreement might affect the decisions we would inevitably have to make about major system changes. A second problem that lurked in the background at first, and then more and more in the foreground, focussed on the question of available time. With ever tightening budgets we found ourselves using increasing amounts of the machine capacity for standard work. There was less and less open time. Should our partner have a disaster and need to use our facilities, we might very well have to interrupt our processing to accommodate theirs. How long could either school be expected to keep this up before the attempt to deal with a disaster on one campus resulted in at least a mini-disaster at the other? The questions were serious questions and hard questions, and most of them never were answered satisfactorily. Although discussions lasted for several years, we never really reached a formal disaster recovery agreement.

It was at this point that we changed our direction. Instead of trying to build a disaster recovery plan which would allow us to reproduce our normal operating schedule in the case of a disaster, we decided to begin building a set of contingency plans that would allow us to continue departmental operations. The difference between the two is important. Our focus in disaster recovery planning had been to find a way to restore the normal operating procedures of the University. Although the changes in locations would be obvious to the technical staff, I think that in the back of our heads we had a vision of the rest of the University continuing along as usual. That picture changed. For the next few months, we decided, we would focus on the critical functions of the University that would be disrupted by a disaster in computing, rather than on the computing itself. After all, it's more important to register students for classes than to register them using computers; it's more important to send offers of admission to prospective students than to send computer-generated letters; it's more important to pay employees than to have automatic deposit of paychecks. For the time-being, our focus changed away from machine problems to operational problems. It became localized, shorter term, of more immediate concern to departments, and we moved out of the role of being the experts to a role of being coordinators and supporters.

The effects of this changes were four-fold. First, we focused on a smaller, easier tasks and as a result increased the probability of success. Second, because the task was smaller and easier to define we were able to gain better control of the costs. Third, instead of trying to solve the big problems, for which I just

don't think we were ready, we gained a great deal of experience in one aspect of disaster recovery planning. We floundered a bit, we made some mistakes, but because of the size of the projects the mistakes were not so overwhelming that we were not easily able to go back and redo those parts of the project. And having learned the mistakes on a small scale, we are now recognizing them more easily on larger projects.
Finally, because of the function that we chose to focus on first, namely payroll, we were able to generate an interest that led to willing, sometimes even enthusiastic, participation.

Preparing the contingency plan was a several step process. In outline the steps were

1. Identify the critical function that had to be continued during a disaster, critical to the operation of he University, not critical to data processing.
2. Review the nature of the disasters that could affect the satisfactory performance of the function.
3. Decide on a plan to ensure the continuation of the function.
4. Test the plan.

We'll look at each of these steps individually.

Payroll involves a lot of details, from collecting time sheets to calculating any of more than a dozen deductions through printing checks and supplying banks with automatic deposit information for employees who choose that option. But the basic issue of all of these was finding a way to get the net pay into the employees' hands on time. That single act was recognized as critical on several counts. For one thing, of course, University employees and their families depend on that paycheck for necessities. For another, at the Strong Memorial Hospital which is the University or Rochester's research and teaching hospital, paying the staff is also a patient care issue. Without the ability to provide regular, assured paychecks to staff, our ability to provide an appropriate level of care also drops. In the Rochester area, there are, for instance, many more jobs for nurses than there are nurses, and many of the hospitals, Strong included, have a significant percentage of the staff working on a contract basis.

The worst disaster that could happen was in which the the computers became unavailable, and even the time sheets from which payroll is computed for hourly employees were destroyed. The paradigm for this is a fire in the computing center 36-48 hours before we process the payroll. The time reports are in ashes; the hardware is unusable; the rooms in which the computers were housed are cordoned off by the fire department; some of our staff members are

hospitalized.

We considered several options to no avail. Outfitting an alternate computer room in the hospital was too expensive; running the payroll system with its large files, multiple options for deductions and complicated record keeping on the small academic computer that belonged to the Simon School of Management was unworkable, contracting with a third party to handle the University payroll involved too great a change from the way we were currently organized. It wasn't until someone suggested that we drive a truck up on the library steps and hand out hundred dollar bills that we found a satisfactory solution. Actually we found two quite different solutions, one for regular employees and another for student employees.

For the regular employees the issue was getting their pay to them. The other tasks usually associated with payroll were not as immediately critical—including computing social security deductions, calculating payments to retirement plans, benefits, IRS deductions. The automatic deposit was not critical. As important as some of those things were, we had more leeway there than we did with the delivery of the net pay.

Moreover, in the scenario that we envisioned, we could not calculate the exact amount that an hourly employee earned, at least not soon enough to do anything with it. The time sheets were gone, destroyed by water or fire and we would have to depend on departments to replace that data eventually. Meanwhile, the best that we could do was to pay the employee our best estimate of the amount due and that, so far as we could tell, was that amount paid in the prior pay period. When we realized that, the solution was clear. After each pay period we would produce a tape containing the employee's name, social security number, division, department, and net pay. A simple program would allow us to use the Simon School computer, the one that was too small for payroll processing as it is usually understood, to print payroll advances on accounts payable checks and along with them to print a check register.

Of course there were questions and objections. What about new employees? They wouldn't be on the prior payroll and wouldn't get advances. We decided that for them we would have to issue hand-written checks, but that was better than writing 8000 checks by hand. What about terminated employees? This procedure would produce checks for persons who should have received their last check the prior period. True, again. If a disaster occurred we would have to depend on the department administrators, the men and women who distribute the checks to the employees, to catch such problems. That meant that we had better

write the letter which would accompany the checks in advance, so that we would not have to remember these details at the time of the disaster. There were other questions, and not all of them arose while we were laying out the plan, but a number of them did.

Unfortunately, the same procedure wasn't a solution for student payroll. For student employees, one period's pay is just not a good predictor of the next. For one thing, the population changes by about one third between any pay student payroll and the next. For another, even for the students who are the payroll for several consecutive periods, the amount that they earn frequently varies by 200%. We decided to approach the problem by expanding on the existing emergency loan program. Currently, students can borrow up to $100 in an emergency, through the Dean of Students' office. They have to pay it back with in two weeks. After a little statistical investigation, we decided that should we have a payroll disaster, we would use an analogous procedure, still overseen by the Dean of Students' office, to lend students up to $200. (That would cover about 95% of the employees on the students payroll—students who had earned significantly more could borrow more if with verification from their employer.) The student had to sign a note, the payment would be due when the payroll was processed and if it were not paid, it would be added to the student's term bill, an action which could eventually block registration or graduation.

This process is a "busy" one. Verifying that the student status, handling the paper-work, and distributing the payments (to be made in cash, remember that the system is down and we don't want to write all these checks by hand and then trace them through the accounting system) involves coordinating the registrar, the bursar, the dean of student's office, campus security, transportation, and facilities, but it does not involve information systems and it does not involve the staff of the payroll department, leaving them free to focus on the employee payroll and other high priority effects of the disaster.

The first test of the employee payroll plan was intended to check several things. First, did all of the steps work? We had, of course, tested the print programs and the productions steps before, but the first full test required people who were unfamiliar with the program and the environment to work on a computer other than the standard administrative machine and print, burst, and sign, deliver, and account for paychecks under emergency conditions. Second, the test provided information about how long it would take us to produce emergency paychecks under this contingency plan. That was information was important to us for we wanted to know the time how much time we would have to decide on strategy in case of a disaster which was not destructive. Suppose, for

instance, that, as once happened, a bulldozer took put the power for the computer center. How long could we wait for the power to be restored before starting the contingency plan? The third set of questions centered around determining if the instructions were clear. Could our staff follow the directions? Where did they have to make decisions? Did they have the information that they needed? Throughout the test we had monitors assigned to serve as timekeepers, to make sure that the test was carried on under emergency conditions (you can't go back to your office for your notes, they were destroyed in the fire), and to follow up with the departments that were included in the test to see that all the telephone call were made and the notices sent.

The week following the test, we met to revise the procedures slightly and to compile a list of issues that arose in reflection on a "live" test that had not arisen around the planning table. We examined the statistics from two consecutive payrolls and discovered that under the emergency procedures, most of the employees would receive within $75 of their correct pay. We also summarized our findings to the president's executive council.

The test was about a year ago. Where have we come since then? Four significant things have happened. A few months after the test we almost had the opportunity to put it into action. A mainframe failure looked as if it would keep us from meeting the payroll deadline and for a few hours we thought that we would be printing "emergency checks." No one wanted to do it, but the staff that had taken part in the test knew that it was possible. Afterward it provided an opportunity for us to review with the senior management paying the kind of attention that they had not previously paid to questions of disaster recovery the issues involved. This also led to a few changes in our contingency plan, including the assignment of one person to serve as liaison between the senior staff and the persons on working on the recovery and contingency plans, for we had learned in our brush with disaster that everyone from a certain level on up was calling to learn the current situation, and, in doing so, interrupting the recovery work.

Nobody really liked the contingency plan. Nobody wanted to use it for the problems that would face us after we issued thousands of payroll advance checks seemed enormous. The clean up of the payroll system, of the accounts payable system, of the ledgers, the problems of dealing with employees who received estimated checks, and the confusions that could arise about the benefit plans appeared to be at least as difficult as the physical clean up of a destroyed computing center. Despite all of our planning, or more likely because of all of the planning, it suddenly hit us that recovering from a disaster was going to be difficult, unpleasant, and costly. That realization led to the second outcome of the

contingency planning. The payroll unit tried to build a microcomputer model of the payroll system that would calculate exact pay due based on hours worked. At first it looked promising, but over a couple of months problems arose that made it impractical. Instead we turned our focus to developing better procedures for cleaning up after the disaster.

The third effort related to the establishment of the payroll contingency plan was the development of a contingency plan for those departments in the hospital which did not have one. Larger than the establishment of a backup payroll system, this project was designed to document operating and recovery procedures for hospital administrative departments and to determine how long they could continue to run using those procedures. The length of time that departments could go without serious difficulties arising from a lack of computer support ranged from three days for admissions and the emergency department to more than a month for a few reporting functions. What was important about his effort, in addition to the plans developed, of course, was the active participation of a large number of persons from across a broad range of responsibilities.

We are now back where we were several years ago, putting together a disaster recovery plan for the University of Rochester. By that we mean a plan which will enable us to last through a long failure of computing at the University and that will describe for us the steps we need to take to restore computing power and the order in which we need to restore computing applications. I expect that we will be able to complete our task less expensively, with fewer hours devoted to it, and with more effective participation than we would have been able to a couple of years ago. To date, a half hour or so with each of the senior executives of the University has enabled us to pinpoint those functions which are most critical to the operation of the University. Some time with the lawyer has given us some answers about other exposures. It is still someone else's responsibility to decide at what level the University requires and can afford disaster protection, but that decision will be made with a good deal more insight into the possibilities than was available several years ago. Collecting the information took about a month and a half; it was primarily a part-time assignment for one administrator who met with a small "direction committee" for an hour biweekly. We expect a report listing exposures and options to be available by the end of the year. Even at this, we are currently looking only at mainframe computing and not at the many departmental systems.

What have we learned? (1) Disaster recovery planning is a big job and demands a good deal of expertise. Start with a small, but critical area to get a feel for it. (2) Planning for disaster recovery effectively means focusing your

attention first on the functions that are crucial to the operation of the university and then, once you have determined those, on the exposures to those functions. (3) A good deal of the ability for effective damage control and continued operation in the event of a disaster comes not from a large scale plan, centrally organized and directed, but from smaller, local contingency plans that have been thought out be the people who do the work every day. Little things seems to make the biggest difference. At the University of Rochester some of the most important things to have available quickly turn out to be lists, easily downloadable on a regular schedule from the mainframe databases, but only if someone thinks about it ahead of time. (4) Planning pays off, not only in case of a disaster, but in keeping aware of the possibilities for current operations improvements.

A Case for Common User Identifiers (CUI's)

Bernard W. Gleason
Executive Director, Information Technology
Boston College
Chestnut Hill, Massachusetts

Boston College has been building and adapting a systems architecture under the label of the User Information System -- an environment in which the individual user (students, faculty, and staff) has the ability to directly interact with university systems. One of the accepted principles of open access to information is the establishment of common user interfaces to facilitate easy access to a multitude of systems. It is equally important to establish common user identifiers CUI's, which are simply data elements that uniquely identify users. This may seem elementary but for many institutions the setting of standards for user identification is still very elusive or disjointed. As access broadens the lack of standards and directory services will further complicate matters.

The presentation will explain the approach that Boston College has taken to develop standards for common user identifiers (i.e. ID numbers, user names, personal identification numbers (PIN's), network node names, ID cards, bar code labels, magnetic stripe encoding, etc.) and the deployment of common log on procedures. The presentation will include demonstrations of how the use of unique user identifiers (ID numbers, PIN's, user names, etc.) are established and maintained in a central directory service, and how these identifiers are used to facilitate the integration of various applications and computing environments. Multimedia demonstrations will focus on the ability to attach a variety of devices and/or interfaces to existing applications while maintaining conformance to the defined common user identifiers (CUI's).

Introduction

Integration has long been a hallmark of information systems at Boston College, and the challenge of the 90's is to extend these distinguishing characteristics to include open access and interoperability. Three years ago Project Glasnost was formally launched; Glasnost being the code word for 'openness' and open access to administrative systems. The guiding principle that has been used throughout the design of administrative systems at Boston College is that of the User Information System (UIS): all members of the community, including faculty, staff, students, prospective students, alumni, and outside agencies must be provided open access to administrative information. Everything we do is in support of the premise that open access is to the benefit of both the institution and the campus community.

Central to our systems architecture is what Bob Heterick from Virginia Tech calls a "single system image". As users become connected to large networks with a mix of vendors, software and communications protocols, there is a need for a single log-on sequence, a single-system access control scheme and transparency between applications. Users should be able to log on to the network and be authenticated just once, instead of logging into separate computers and applications with separate procedures. The key is the establishment of a name directory that will permit a single log-on capability for users. The User Information System is designed so that the user views a single system which can be customized to individual needs with the appropriate functionality, and one of the accepted principles of open access is the establishment of common user interfaces to facilitate easy access to a multitude of systems. It is equally important to establish common user identifiers CUI's, which are simply data elements that uniquely identify users.

As soon as an individual is identified through the transactional system as being associated with Boston College as an employee or student, the User Information System (UIS) automatically generates common user identification information. Usually the first action of a new student or employee is to obtain a University ID card, which contain the unique common user identifiers (CUI's) of name, facial image, ID number, bar-code label and an encoded magnetic stripe. This card serves as a passport that has universal usage across campus. (The investment in an information system should not be measured solely by the initial cost of the systems development effort, or by the usefulness of the system to service the primary user offices. The real payoffs come when the facilities in the system architecture are fully exploited or used by other applications within the User Information System. For example, many universities issue a single identification card to every student, faculty member and employee, while others issue different ID cards for different application systems. The benefits of a single ID card in terms of lower production costs and increased utility across many applications are obvious.) At the time that the ID card is produced, the UIS also automatically

generates the unique common user identifiers (CUI's) of username, password, and Personal Identification Number (PIN) for each individual. This set of unique identifiers collectively form the common user identifiers (CUI's) that are utilized by all applications in the UIS. The following is a list of common user identifiers that are unique to each user and are utilized to control access to the system and to automatically associate individuals in a variety of ways:

ID Card
Person's name
Facial image
ID number
Magnetic stripe
Bar Code Label
User Name
Pin numbers
Passwords
Position (Job) number(s)
Building/room number
Telephone Number
Network node name
Vehicle tag number
others.....

Central Directory Service

Common user identification information, security profiles, and demographic data for all individuals associated with the institution are stored in a central directory which forms the basis for directory services functions. The campus telephone directory is extracted directly from the UIS just prior to publication, and this directory is also available on-line in all computing environments as one of the standard menu functions. Usernames are unique and each user has a primary mail address. If the user has mail addresses on multiple machines or servers, the user name is the same in all environments and is known to this central directory. For example, I'm GLEASON on all Boston College systems (mainframe and departmental) on which I have an account, but my primary mail address is on the departmental server.

The central directory can be viewed as a collection of business cards for everyone affiliated with the university, including students. Like the business card, each directory entry contains name, title, campus address, telephone number, electronic addresses (user name and node), FAX number, and all of the common user identifiers. By employing a central directory service, it is not only possible to interconnect electronic mail systems into a single system,

it is also feasible to consider using a single identification to access all messages, whether they are voice, text, or facsimile.

Common User Identifiers (CUI's)

Common User Identifiers (CUI's) are stored in a central directory service that is dynamically maintained by data supplied from administrative production systems. For example, the human resources system at Boston College contains a position control function, and as individuals are hired, terminated, or change positions, the system automatically assigns position-specific attributes, such as office location, telephone number, job title, and so on to the individual. In addition, the system assigns the access control profile associated with the job. Individuals may hold multiple jobs, or may attend classes in addition to being employed. At the time that an individual becomes associated with the university, or changes status within the university, his or her information is entered as a normal transaction function into the system (human resources or student record systems) which automatically alters the individual access control profiles that are associated with the individual. The person's personnel and/or registration records determine the individual's group or class assignments.

At log-on execution, users are allowed to gain privileges in one of five ways: by groups or classes to which they belong (i.e., faculty, staff, and students); by responsibilities associated with specific jobs; by individual (for access to his or her own records); by data dependency; or by organizational structure. At that time, the system applies the rules and develops a set of user profiles. The access control facility will then map all of the appropriate profiles together so that a composite of the individual's privileges is recalculated at the start of each session. This user profile can be accessed by any of the unique common user identifiers.

The hierarchy of departments and positions is defined within the system, and individuals, by virtue of occupancy in a position, may have access to information that is available to individuals in positions lower in the structure. For example, access to budget information for a grant in the biology department should be provided to the principal investigator by virtue of his or her job responsibility. The dean of the college, who may be seven or eight levels up in the hierarchy, may not be directly responsible for the budget, but would have authority to access the budget information using a workstation or telephone voice response.

Individuals have access to their personal records on a one-for-one relationship. For example, a student has access to his or her student account, financial aid, grades, and other records; employees have access to their own personnel, payroll, and student records. Individuals also have access to records based upon the data resident in records in the production systems. For

example, a faculty member has access to records of individual students for advisement based upon the registrar's designation of the faculty member as the advisor in the student's record.

Personal Identification Numbers (PIN's)

The changing of passwords on a regular basis is one of the standard controls in most security systems. In an environment where users are constantly accessing a system, this procedure works well. But if there are many infrequent users, then there is a different set of issues. Infrequent users will often write the password on a piece of paper, or will be discouraged from using the system because either they can't remember the password or it has expired. With large numbers of users, this can cause a logistical and administrative nightmare.

It is interesting to note that banks do not require users of ATMs to change passwords on a regular basis, even though unlawful access could result in the theft of cash. It is likely that the banks have concluded that it is better not to require frequent changes if by not requesting them, customers will be discouraged from writing passwords on their bank cards or on pieces of paper in their wallets. The same logic is applicable when dealing with limited access to information by the entire university community. This is accomplished by providing a unique PIN to all owners of a campus ID card at the time that the card is issued. Because the PIN is unique, it also serves as another student, faculty or staff ID number. The PIN can be thought of as a "half a password" that provides the first level of access control, determining the menu of services available to the users. Passwords and associated restrictions are required for deeper-access privileges.

The concept of the PIN also differs from passwords in another significant way. Just as the student, faculty member, or staff member will use the same ID card to access many application systems, the individual will also always use the same PIN. The repetitive use of the PIN in many applications makes it easy to remember, and at the same time, serves better than other possible qualifiers, such as birthdate.

On most campuses, servicing of students in the library and public computing facilities, as well as normal access to computing networks, is nearly a seven-day/twenty-four hour proposition. Students should be able to utilize the services of the network not only for course work, but also to access administrative systems, similar to the way we now conduct our banking business. Since the lifestyles of students are not synchronized with the standard Monday-through-Friday, 9:00-to-5:00 office hours, at Boston College, they have the ability to conduct business with the administrative offices of the university beyond normal working hours. For example, students can retrieve grades, review their student account, register for courses, and print

course schedules by gaining access to the central directory and access control system in the UIS.

All institutions are not likely to attain complete integration of all systems, but it is still important to develop a perception of a single system. The use of a common access control identifier, such as user name, is one important component; another is to provide consistency in naming systems. For example, all systems at Boston College are referred to as the U-Series, where "U" stands for user, which implies that all the sub-systems are integrated and user-focused. The voice response registration system is called U-Dial, the purchasing system is U-Buy, the ATM student information access system is U-View, the food service system is U-Dine, and the electronic mail system U-Mail, and so on.

Multiple Access Methods

The design User Information System permits access to information from multiple device types. In cases where the telephone is used to interact with the system, the application is designed to function the same on all platforms, with the telephone keypad being the lowest common denominator. This design is referred to as the RISK, or Reduced Instruction Set Keyboard, technique. An example of this type of application is student course registration drop/add. In this application, the user is restricted to numeric entries (i.e., social security, PIN, course numbers, and selection and response keys) and function codes (i.e., star and pound signs). The terminal operator in the registrar's office with a full-function keyboard uses the same limited keyboard functions and numeric entries, and the same is true for a student processing the transaction using an ATM-type device, which utilizes a keypad similar to a telephone.

The following are examples of the use of CUI's in providing students with access to a student information and registration application using multiple access methods. In all cases, the underlying data structures and applications remain unaltered, the front-end device and the presentation vary from application to application.

U-Dial — Student registration and course drop/add using a telephone and Voice Response Unit (VRU). Student ID number and PIN used as CUI's to log on.

U-View ATM — Student information retrieval and course drop/add using a device similar to an Automated Teller Machine (ATM). Student ID card, magnetic stripe and PIN used as CUI's to log on.

U-View 3270

Student information retrieval, registration and course drop/add using an IBM 3270 terminal. For example, students can select the U-View application from the main menu of public access terminals in the library catalog area. Student ID number and PIN are used as CUI's to log on.

U-View VT100

Student information retrieval, registration and course drop/add using any VT100 terminal. Students can access the application through the VAX Cluster. Student ID number and PIN are used as CUI's to log on.

U-View Macintosh

Student information retrieval, registration, and course drop/add using a graphical front-end on an Apple Macintosh. Students can access this application from any Macintosh in the public computing labs. Student ID number and PIN are used as CUI's to log on.

U-View Dial-in

Student information retrieval, registration, and course drop/add using a Macintosh front-end that contains built-in terminal emulator. Student ID number and PIN are used as CUI's to log on.

NOTE: Each of these methods will be demonstrated during the presentation using multimedia techniques, including color, animation, on screen video, audio annotation, and screen capture.

By permitting users to access the UIS from a multitude of devices, we are not only providing users with the ability to access information in the most convenient manner but we are also addressing the problem of bottlenecks that commonly occur if an application can only be accessed one way. For example, if the single method application is an on-line registration and drop/add system, there may still be long lines, or if the method is dial-in registration, then there may be problems with jammed telephone circuits.

Integrated Applications

The availability of a central directory service that is a repository for common user identifiers facilitates the ability to integrate application systems and various computing and communications environments. In conjunction with the directory, the UIS is designed to easily employ intelligent routers. These routers are composed of a set of tables maintained by custodial user

departments and allow a user to execute mail or forms-routing transactions without stipulating the receiving party or parties. The identity and the address of the recipient is determined by using CUI's to access the central directory service. The system uses a mechanism to provide the user with transaction-generated messaging by having intelligent agents which know "who should know what," and automatically triggering messages or reports based on activity. This feature alerts individuals on a timely basis, rather than requiring the user to execute queries. For example, this facility automatically generates an electronic mail message to a professor alerting him or her to a student's withdrawal from the professor's course. In traditional database environments, we have written systems that communicated on an application-to-application basis, i.e., one program sending data to another program. In electronic mail systems, the communication is usually peer-to-peer, i.e., an individual sending a message to another individual or group of individuals. In the integrated database/mail environment, applications talk to peers and peers to applications, using CUI's to determine the identity of the peers.

Individuals are also able to initiate mail by addressing the message to a group and utilizing automatic distribution capabilities. For example, a professor can address a class assignment to all students enrolled in a course, as long as the system determined that the professor issuing the memo is also the instructor. If authority is granted, the system uses the class list to determine the students and the corresponding directory entries to determine the appropriate mail addresses and routing schemes. The system accepts messages and forms from different computing sources, and a single routing scheme is utilized for distribution of all messages and forms to a single desktop mailbox. Users who do not have an electronic address or who do not read messages within a prescribed time limit receive a printed copy automatically through campus mail.

Despite the growth of networks and permeation of desktop devices, the telephone remains the ubiquitous communication device in the home and office. The convenience of the telephone permits documents to be transmitted using a FAX machine, and the telephone has gained acceptance at colleges as a means to register for courses from their homes. In many instances, voice and data are being serviced over the same medium, twisted-pair wiring, and telephone switches and computers are gaining a higher degree of integration. The UIS is currently being adapted to support integrated voice and data services through a common set of controls that will manage access to both network and information resources. Included in the plans are the integration of electronic and paper campus mail facilities with the voice mail system, so that users can be alerted to entries in their voice mail boxes from the electronic system, and vice-versa. When a user provides a PIN number to the telephone system for long distance access, it will be the same PIN number that is used when logging on to the data system, and

telephone access security and privileges will be managed by the same security routines and techniques. The UIS will also support the integration of databases and telephone services. For example, at help desks the data base record of a caller will automatically be displayed on the screen. Users will also be able to access administrative systems information through the use of a touch-tone phone. For example, a department manager will be able to check on the status of a budget by entering an authorized account number, and prospective students will be able to check on the status of their applications. The system may support both stored and synthesized voice applications, and the selection of the appropriate technique by the system integrator is based upon the audience. All systems will be designed with date and time stamp functions so that users can perform status checks using either voice response or workstation access.

Conclusion

At Boston College, we have developed an integrated systems architecture, which provides a platform on which to build all applications, and which enables campus-wide data sharing. The User Information System can be characterized as interactive, integrated and highly standardized. The application of standards includes screen formats, program structures, naming conventions, data definitions, access codes, and common user identifiers, resulting in a consistent user interface across all systems. Most importantly, the single systems architecture, the single directory, the single access control system, and the data requirements are all complete. In a sense, the hard work is all done, and as new technologies become available from vendors, we will simply attach the appropriate services to the system as component parts.

The establishment and maintenance of common user identifiers is a common sense approach to the setting of standards. The conformity to standards and a single architecture has provided some obvious technical benefits, but it has also furnished a base for providing a true end-user computing environment characterized by ease of access and intuitive interfaces.

A WORKING MODEL FOR MANAGING DATA STANDARDS AND POLICIES IN AN INTEGRATED DATABASE ENVIRONMENT

ABSTRACT

Two years ago, Bentley College established a Data Standards and Policies Committee to develop, monitor and maintain clear policies and procedures for the collection, integrity, use and disposition of data maintained on the College's centralized administrative database. This group, the successor of several unsuccessful predecessors, has worked quite effectively since its inception. Our paper reports the background for the establishment of this Committee, its structure and operations, with examples of issues it has encountered and has resolved during the past two years. We hope it can serve as a model for other institutions in dealing with issues of data standards and policies in complex centralized database environments.

Peter T. Farago
Director of Institutional Research and Planning Studies
Bentley College

Jessica Whitmore-First
Manager of Data Administration
Bentley College

Presented at CAUSE90
Miami Beach, Florida
November, 1990

A WORKING MODEL FOR MANAGING DATA STANDARDS AND POLICIES IN AN INTEGRATED DATABASE ENVIRONMENT

Peter T. Farago and Jessica Whitmore-First
Bentley College

The Need for Data Standards and Policies

Since 1983 over 300 users in 30 offices at Bentley College have shared data stored on a PRIME INFORMATION database using the administrative systems package AIMS. Additional offices, while not having direct access to the data, require indirect access to it to perform their functions. The AIMS system is maintained by the Administrative Systems (AS) Department with an applications programming staff of up to 16 programmers.

During the past seven years, the AIMS system has been modified beyond recognition and new functionality was added to accommodate several offices.

During this same time period, a number of offices abandoned the AIMS system because they considered its functionality inadequate. Some offices quietly left the AIMS system because the data that they required were in a form that was inappropriate for them.

A fair number of offices discovered ways to circumvent the AIMS system when it failed to satisfy their needs. For instance, some offices devised means to store information on the system when there was no previously designated location for the data.

Frequently, information on the AIMS system was maintained and used by one office, but was also required by other offices. It was not uncommon for data to be referred to, and thought of, as being "owned" by the office that entered and maintained the information. In some circumstances, the "owner" and the other users of a particular set of data negotiated an agreement for sharing the information. However, in many other cases, there were disagreements regarding the access and use of information "owned" by one office and required by others.

When the "owner" of a particular set of data was unwilling to share that information with other offices, AS would be asked to intervene by either convincing the "owner" that the request was reasonable, or by quietly arranging access to the information.

At times, user requests were made to AS that, if implemented as specified, would

seriously have compromised the integrity of the database. Consequently, the AS staff was obliged to reject these requests.

The AS department was perceived by many users as wielding total control of the administrative computer systems. These users presumed that the AS staff unilaterally determined which offices had access to the information stored on the system, how each office gained access to the data, and when the information would be accessible. Correspondingly, these users expected the AS department to protect their data from "undesirables".

AS was seen as the police officer, judge, and executioner; an unenviable position for any office to be in.

The Search for a Workable Solution

The basic problem encountered with the AIMS system was twofold: the people with sufficient knowledge did not have the authority to make decisions, and the people with authority did not have the knowledge to make the best decisions.

Starting in late 1983, when Bentley College was implementing the new AIMS system, two committees were created. In part, these committees were formed to resolve the problems and issues that arose from establishing an integrated database system. One committee, the Administrative Systems Planning Committee (**ASPC**), was comprised of directors of various administrative offices from across the campus. The second committee, the Information Services Steering and Planning Committee (**ISSPC**), consisted of the institution's Vice Presidents.

ASPC's mandate was to resolve controversial issues. However, the member's of the committee typically failed to agree amongst themselves. Most of the members did not have sufficient knowledge to make an educated decision, and were required to rely on their staff to understand the possible ramifications of their decisions. This process was time consuming, and an incredible bottleneck developed. In addition, internal college politics often consumed the committee as most issues evolved into turf battles. When the committee failed to reach an agreement, the issue in question was elevated to the VP's ISSPC committee.

The VP's, however, were even less equipped than the ASPC members to make educated decisions about data administration issues. Consequently, some of the issues presented to the ISSPC committee were tabled for months as the VP's acquainted themselves with the issue and the various interested parties lobbied for their preferred resolution.

This alternative was definitely not working.

In late 1984, a new group, Data Administration (DA), was formed within the Administrative Systems Department to handle the day-to-day issues that arose from the operation of an integrated database. Unfortunately, the users of the system, as well as the administrative systems staff, were hesitant to embrace this new group. The function of the DA group was not clear; the group was to manage the data, but to what extent?

In Ken Brathwaite's book, Data Administration: Selected Topics of Data Control, many possible definitions of Data Administration are presented. One definition, borrowed from M. L. Gillenson, is a broad description of data management:

> "[It] includes data-related planning, liaison to systems analysts and programmers during the application development process, training all relevant personnel in data administration concepts and techniques, standards setting and monitoring, database and possibly even application design, documentation...usage authorization, arbitration of disputes over access authorization and database system performance, change impact assessment..."

With all of the above functions as possible activities for the new DA group, one can see why people might be concerned about the impact that DA could have on the user's accessibility and control of the system. Many feared that the new group would involve themselves in everything, and become another huge bottleneck.

The end-users were also concerned that, since the DA group was in the AS department, the DA staff would have biased views and agendas that were opposed to those of the end-users.

Issues regarding the use and misuse of data constantly were identified by the new DA group. Many of these issues were potentially damaging to the system. Unfortunately, while the DA group had the knowledge and system rights to correct the problems, the group lacked the authority to implement necessary modifications to the system. Like ASPC and ISSPC, Data Administration was not the proper group for the job.

Examples of the type of problems experienced on AIMS:

Example 1. Human Resources

Human Resources (HR) is responsible for capturing and maintaining personnel data. HR quit the AIMS system due to concerns over system security. However, certain personnel data, (e.g., campus address, current employee status, and emergency contacts), which had been maintained by HR were also used by a number of other

offices. When HR abandoned the AIMS system, they informed Administrative Systems that they would not pass new or changed information to other offices.

Maintaining employee addresses, locating employees in emergencies, generating mailing labels, verifying employment and countless other functions now all had to be routed through HR as data on the central system became unreliable. Management reports or analyses requiring HR data merged with other system data (e.g., faculty workload analysis) became impossible to do. Multiple, alternative and disparate personnel files began to be maintained by offices around campus, each for their own use. The advantages of a common database were lost, and people couldn't understand why AS couldn't just "fix" this.

Example 2: Duplicate Records

Since its installation in 1983, the AIMS system has had duplicate records. When Institutional Advancement (IA) was converting to their new system, they did not want any duplicate Alumni/Development records transferred to the new system. Therefore, the IA staff carefully reviewed the AIMS Alumni/Development population to identify any duplicates. When a duplicate was located, IA chose those records that had contributions posted to them. The duplicate record without contribution activity was designated as the "bad" record, and any pertinent data was merged into the "good" record. The "bad" record would then be deleted from the Alumni/Development portion of the database. This still left the "bad" ID on the main database with it's information potentially spread across scores of files.

To ensure they never saw the bad record again IA removed any information they could from the main database file for these records. In addition, they replaced the first line of the "bad" record's address with "Duplicate of number ##" (## referring to the good record in the database). IA was confident that none of the merged records were active Bentley students.

Some months later, the registrars in Bentley's three schools, were processing fall semester correspondence for their active students. Some of their mailing labels, however, were printed with a strange message in the first address line. Obviously, the registrars were up in arms, angered over the fact that "anyone" could erase information on their students from the database.

Over the next week, the DA group worked about 25 hours to restore backups and recover the lost data. In addition, the registrars had to manually identify which students had been affected. Demographic information from the "good" record could not simply be added back into the "bad record. It was usually the undergraduate record that had contribution activity, and it was very common for an undergraduate student's address to differ from their current graduate student address. Complicating

the situation was the fact that IA had erased a critical data field that the registrars needed to easily identify current students and had done so over a 4 month time period.

Here was another instance where procedures, policies and controls were needed, What was lacking was the entity with both the authority and the technical ability to put these in place, or with the political persuasive power to have these accepted by affected user groups.

The Solution

The latest, and so far most successful, attempt to form a committee with both the knowledge to determine the best solution to data issues and the authority to develop and implement strategies and policies to address the issues came two years ago.

A Data Standards and Policies Committee (DSPC) was formed under the direction of the Vice President of Information Services. To quote from the VP's announcement:

> "...With the use of large complex databases...have come some unavoidable problems. Many of these problems have to do with what data are collected, who has the responsibility for collection, maintenance and integrity of the data, who may access, and use the data in what ways? Often these issues can be resolved among users and data base administrators. However, occasionally instances occur when different interests of offices conflict, or the issues need a broader institutional perspective. At other times institutional policies may be involved...These types of data and policy issues are best handled by an independent entity which combines technical understanding with an overall institutional perspective to balance the benefits against the costs of alternative policy options."

Indicative of the controversial nature of the mission of the DSPC, this official announcement was not distributed to the Bentley community until almost one year after the committee was formed and began its work.

Structure for Decision Making

The initial charge to the Data Standards and Policies Committee was extremely broad. Most importantly, The DSPC was to make decisions on data issues with the goal of maximizing the benefit to the institution as a whole, but not necessarily the benefit to any one operational department.

Within this broad context, the specific charge of the DSPC committee was to:

1. Ensure the existence and use of consistent data standards for all administrative computer systems.

2. Establish policies for data capture, maintenance, ownership and access, in particular in those instances where these issues concern several operating areas or where conflicts of interests among parties need to be resolved by an independent decision making group.

3. Ensure the availability of a reliable, complete data base for operational as well as for management information, institutional research and planning functions.

4. Monitor and ensure the integrity of the various data files by conducting periodic data audits.

5. Develop policies for data retention, archiving, and purging.

6. Support the conversion of various systems through the review of table definitions and coding schemes to assure their consistency, usefulness and completeness from an institution-wide perspective.

The role of the Data Standards and Policies Committee sounded very similar to the "classic" role of Data Administration. Once again from Brathwaite's Data Administration: Selected topics of data control, we are given one concept of Data Administration which sounds remarkably like the charge of the Data Standards and Policies Committee:

> "[It] is the establishment and enforcement of policies and procedures for managing the [college's] data as an [institutional] resource. It involves the collection, storage, and dissemination of data as a globally administered and standardized resource."

Because of the overlap with similar responsibilities usually assumed by Data Administration, it was important to have a close relationship between this committee and DA. A key to this arrangement working smoothly was for the committee to avoid trying to do the job of data administration. Keeping this distinction, that is keeping the committee focused on policies and standards, and letting DA handle the implementation of these was crucial to avoiding either of these two groups trying to do too much, or trying to do each other's jobs.

The second key to the success of this group was its composition. The criteria for

selection were that the person be familiar with how data are used in their respective areas, that they be key operational people in their offices, i.e. they had to be people who would be listened to within their own areas. A more subtle but maybe the most important qualification was that they be the persons with the greatest personal investment in the availability of reliable data, or put more bluntly, those whose lives are made most miserable when any data problems occur. These criteria gave us a group (larger than we originally expected) of highly capable, knowledgeable and dedicated middle managers from various user departments. (See Figure 1.)

The selection of the Director of Institutional Research to chair the committee, was intended to insure at the outset that neither DA nor a particular user group in the College would be perceived as dominating or controlling this group. Our contacts with colleagues in similar institutional research positions at universities and colleges nationwide indicate that an increasing number of them are being called on to play similar roles in their institutions. The reasons for this include their position as sophisticated users, their familiarity with multiple parts of the system, their personal need for and interest in the existence of accurate and reliable data for analysis and management information, and their institution-wide view.

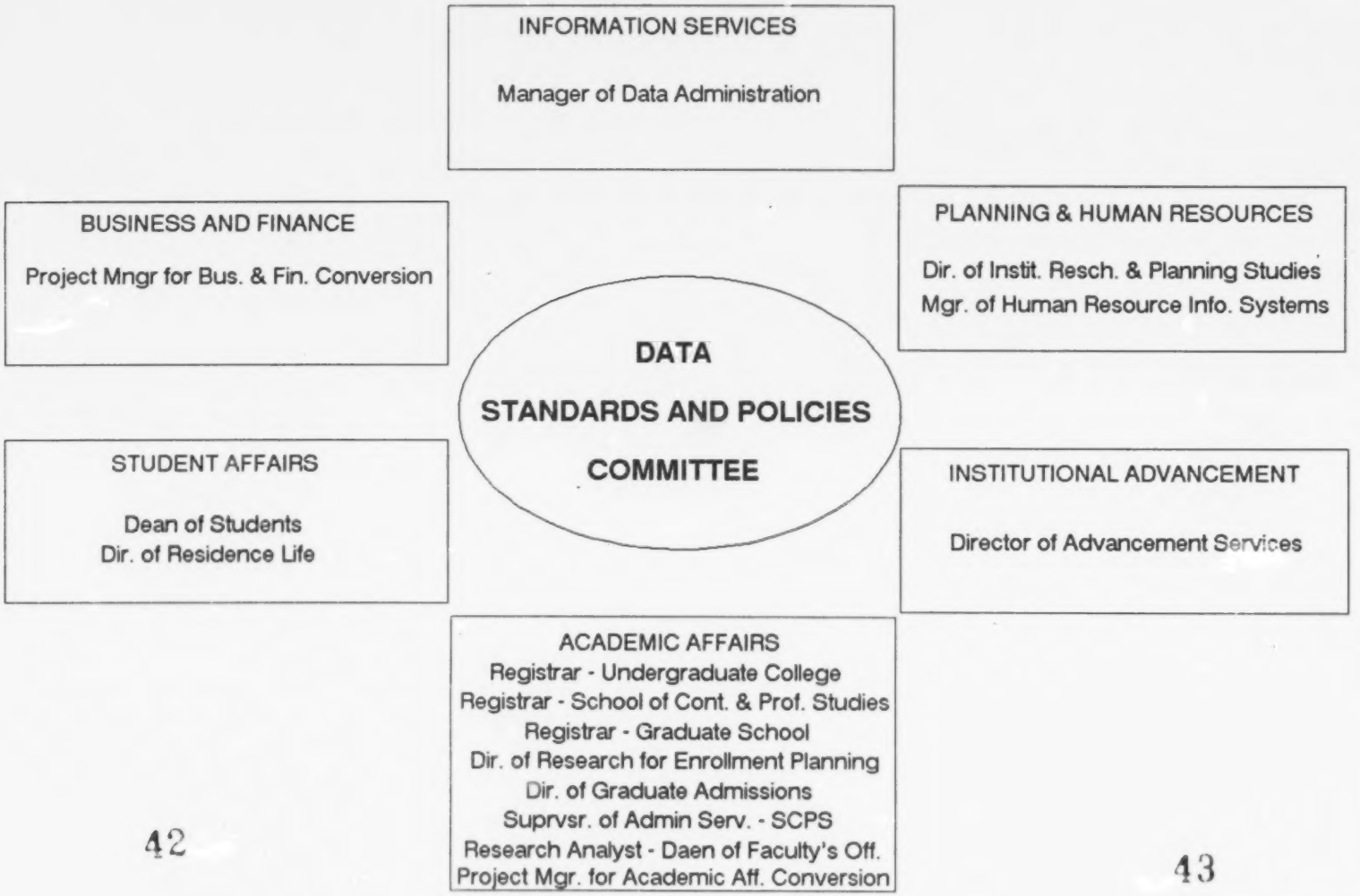
Formally, at Bentley College, this committee reports to the Vice President for Information Services. This is a logical pathway for bringing institution-wide issues and policies to the attention of the top executive level of the administration. One of the circumstances which has made our committee function successfully during the past two years has been the relatively hands-off role of the Vice President. While he has not been reluctant to express sometimes strong views on certain issues, to date none of the decisions of the committee have been reversed, even when they did not match the Vice President's personal preferences. This fact has strengthened the committee and if anything, the knowledge that their decisions will be taken seriously, has made the group more careful and deliberate in its decision making when dealing with controversial issues.

The Process of Decision Making

The procedures of the committee evolved during the past two years. The committee meets regularly and frequently. Weekly hour and a half meetings at a set time are the routine unless there are few or no agenda item ready for discussion, in which case the meeting is shortened or canceled. The norm is to meet weekly, but not to waste people's time unnecessarily. Minutes are kept and written up each week. Guests are invited from time to time as needed from various user offices or support areas (e.g. internal auditor, legal advisors).

The decision making process itself is often slower than some would wish. However,

MEMBERSHIP OF DATA STANDARDS AND POLICIES COMMITTEE


INFORMATION SERVICES
Manager of Data Administration
BUSINESS AND FINANCE
Project Mngr for Bus. & Fin. Conversion
PLANNING & HUMAN RESOURCES
Dir. of Instit. Resch. & Planning Studies
Mgr. of Human Resource Info. Systems
DATA
STANDARDS AND POLICIES
COMMITTEE
STUDENT AFFAIRS
Dean of Students
Dir. of Residence Life
INSTITUTIONAL ADVANCEMENT
Director of Advancement Services
ACADEMIC AFFAIRS
Registrar - Undergraduate College
Registrar - School of Cont. & Prof. Studies
Registrar - Graduate School
Dir. of Research for Enrollment Planning
Dir. of Graduate Admissions
Suprvsr. of Admin Serv. - SCPS
Research Analyst - Daen of Faculty's Off.
Project Mgr. for Academic Aff. Conversion

42

43

FIGURE 1.

this is because the issues rarely are as simple as they initially seem. Often procedures and operations of several offices are effected, and in some cases deep philosophical differences exist about how people view issues. We strive for a consensus, but are willing to make decisions by majority rule if a consensus is not possible. The possibility (threat?) of a majority decision sometimes can make compromising to reach consensus a more attractive alternative. Dealing as we are with technological issues, we often find that the technology can be modified to give us a solution option that most of us can live with and be comfortable with.

The time commitment for members of the committee can be a problem. As key people in their respective departments, the committee members are generally very busy people. Two things appear to be important in keeping people active and committed. One is that things get accomplished. Decisions, although sometimes lengthy are made, closure is brought from time to time, and real operational issues and problems are resolved. This is essential the making members feel that they are not wasting their time. The other important element is an atmosphere of camaraderie. We feel that we not only suffer together through endless meetings but we also have a level of understanding of each other's issues which often we do not find from anyone else in our own areas or departments. It's nice to be able to talk about data and systems issues to others who can understand and appreciate our problems. Getting help makes us all more willing to give help, in spite of our already busy workloads.

Sampling of Issues Considered

The following are some examples of the various types of issues which the Data Standards and Policies Committee has encountered during the past two years and the way the committee resolved each.

Issue: Instances of invalid codes occur in database, as a consequence of unedited loading of data.

Resolution: DSPC asked the Data Administration staff to run audit programs and reports results to the Committee. The Committee reviewed and authorized changes and edits to be made (global or individual) after assuring that changes will not disturb any operational function on campus. Data administration then performed any necessary backups, executed the authorized changes, and repeated the audit after the changes were made.

Issue: Duplicate coding schemes for faculty ranks were found to be used in the system.

Resolution: Independent parts of system were found to use different coding schemes for faculty rank. Data administration was asked to perform audits of the data. DSPC agreed to and authorized a new uniform coding scheme. Administrative offices agreed to inform faculty and staff about the changes to the new coding scheme. Data administration performed backups, executed the recoding of the data in the database and repeated the audit after the changes were made.

Issue: New data code tables had to be set up in the course of the conversions as we migrate to a new software system.

Resolution: All new data code tables for new system are passed through DSPC for review and approval. Changes are often suggested and made. Any subsequent changes are also passed through DSPC. DSPC maintains log of all approved data code tables and their successive iterations.

Issue: An institutional policy decision was needed concerning the use of either social security number or generated numbers for student ID.

Resolution: The Data Standards and Policies Committee examined the effects of alternate schemes on the problem of duplicate records, reviewed the literature of arguments for and against use of Social Security numbers as ID. These arguments pro and con were discussed at some length, including a soul searching deliberation over issues of privacy. Technical capability of our systems were explored for alternative options. Finally, the decision was made to use generated ID's while maintaining Social Security numbers on system separately, and having all ID searches run against both fields. Thus minor technical changes to system procedures allowed us to come up with a policy which everyone could accept.

Issue: Institutional policies and procedures were lacking or confused concerning the use and release of student directory information for internal use, to student organizations, to faculty members, to the general public, and to outside vendors, agencies and organizations.

Resolution: Policies and procedures were discussed and developed by the Committee based on the varied experiences of the departments represented by committee members. The Committee then developed informational materials to advise the user community concerning these policies and procedures. New forms were designed to allow for audit trail for data release requests and for signoff by requestors acknowledging restrictions on the use of released materials.

Issue: Institutional policies and procedures were needed to insure security and control of system data code validation tables and edit rights to these tables for various users.

Resolution: System data code tables were differentiated based on the needs of users for frequent additions or changes to code tables. Some tables, designated "closed", could not be changed by anyone without prior approval from DSPC, and then changes were to be made by data administration only, following standard procedures for backup and other checks. Some other tables, those requiring frequent changes and used primarily in only one functional area, were designated as "open". A limited number of users were granted rights to add codes to these "open" tables or change code description, with subsequent notification of DSPC. Removal or changes to the codes themselves in these tables must still have prior DSPC approval and pass through data administration's routine audit, backup and change procedures.

Data Administration's Reactions

It is no surprise that the DA group has been very pleased with the formation and success of the DSPC, a body with the power to decide controversial issues. The DA group supports the committee as researcher, analyst, implementor, and documenter, but not decision maker. Definitely, DA has had views regarding most of the issues that have come before the committee.

The establishment of the DSPC has given the DA group another chief. The committee decides how an issue should be resolved, and DA implements the resolution. Frequently, DA must collect background or baseline information for the committee as they review an issue, and when a decision has been made by the DSPC, the DA group must prepare and implement the database or system modification. Many times, the DA group requires more time to research an issue or implement a modification than is needed by the committee to resolve an issue. It is not uncommon for DA to delay the resolution process as it gathers information for the committee.

Committee Members' Reactions

The committee sometimes sees itself as taking too long to resolve issues, particularly those of a controversial nature. In its defense, the committee must revisit an issue many times before all of the necessary people have become involved, the information has been gathered, and all aspects of the issue have been analyzed.

In addition, the ramifications of some decisions by the DSPC are quite significant. There may be major, behind the scene changes that need to be completed to

implement a committee's decision. There often is a great deal of preparation work that must occur for a decision to be successfully implemented.

None of the committee members had any of their other responsibilities reduced when they joined the DSPC. Committee assignments must be squeezed into already tight schedules, making it difficult for the members to complete the work of the committee.

Conclusions and Future Directions

The Data Standards and Policies Committee at Bentley College has worked well during the past two years. One of the chief spinoff benefits from this committee is a heightened awareness and realization on the part of key users of the complexity and the interdependence of the system which they use. The members of the committee have matured from having a parochial view of the system to a much more global appreciation. In addition, the committee has provided a somewhat unexpected forum for discussion and airing of some very different and valid views concerning such issues as privacy rights, data ownership, the tradeoff between security and user flexibility, and the need to educate the broader user community concerning the use of data to which more and more of them now have broad access.

Future directions for the committee will include policies concerning archiving and purging of data (so far usually avoided by just upgrading hardware capacity and power), other security issues, as well as the routine work of assuring the integrity and accuracy of the exploding volume of data maintained on our systems.

Adding Value: The Role of Documentation in Application Development

Donald E. Heller, Director
Joan Perkins, Manager of Documentation Services
Steve Csipke, Editorial Supervisor

Administrative Systems Development

MIT Information Systems
Massachusetts Institute of Technology
Cambridge, Massachusetts
November 1990

Is documentation important? How does documentation fit into application development? This paper discusses the changing role of Documentation Services, part of Administrative Systems Development (ASD) at the Massachusetts Institute of Technology. Originally, Documentation Services supported the central development department (ASD) and the client base — always on call, always available. However, two years ago ASD adopted a structured application development methodology for projects and implemented a chargeback system for working with clients.

While clients still want their user and technical manuals, they are more careful about defining what they need and how they will use it. And Documentation Services must demonstrate that the perceived costs of producing manuals during the development cycle will actually save money later, when the application is in production and during maintenance.

This paper approaches the value-added role of documentation from three perspectives: the director of ASD who led the change in organizational focus, the manager who markets writing services and develops projects, and the editorial supervisor who enforces standards and makes sure the client gets what is needed.

Introduction

A key part of the development of any computer application is the documentation. Documentation can include various products: user manuals, programmer reference manuals, system manager procedures, training guides, on-line help. As more and more people in a university use on-line computer applications, and as those applications become more functional and complex, the need for thorough, effective documentation is being recognized more universally.

The Massachusetts Institute of Technology (MIT) is a large research university with a diversity of administrative computer applications. In its last fiscal year (July 1989 – June 1990), MIT spent $19 million on the development, maintenance, and operation of administrative computer applications. Over the last decade, MIT has gradually distributed the responsibility for the development, maintenance, and support of these applications from a central group to many of the business units who are the custodians of the applications. Today, application development is divided about evenly between departments who provide their own application support (through either their own staff programmers or outside consultants) and those who use the central group, Administrative Systems Development (ASD). Figure 1 below shows how the costs for administrative computing were distributed among the major administrative areas of the Institute.

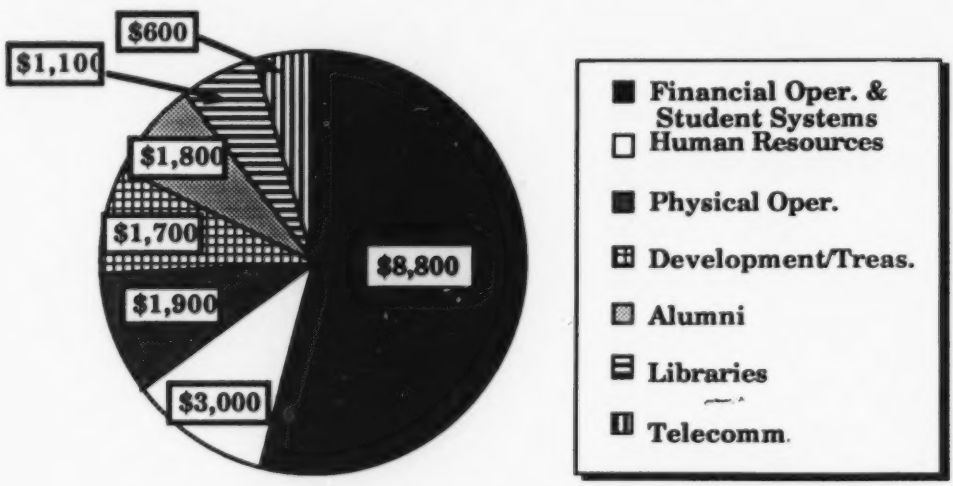


Figure 1. Administrative computing costs by area, fiscal year 1990.

In addition to having an environment of distributed responsibility for administrative systems, MIT also has a heterogeneous technical environment. Administrative, or business, computer systems run on IBM mainframe computers, Digital VAX computers, and Apple and IBM personal computers. Database management applications include ADABAS, Ingres, and Oracle. Many older applications use VSAM and RMS "flat files". For communications, the majority of administrative users rely on point-to-point communications from either dumb terminals or personal computers in terminal emulation mode. Some people take advantage, however, of MIT's TCP/IP campus spine network, which has many DECnet, Novell, and AppleTalk local area networks connected to it.

The Traditional Approach to Documentation

In the last few years, ASD has implemented both a chargeback mechanism for its services and a structured application construction methodology. These changes, when combined with the partial distribution of responsibility for application support, have affected how ASD provides services to its clients and the role of documentation in an application development project.

Prior to these changes, ASD's predecessor organization was responsible for the majority of administrative application development work at MIT. All of its work was funded centrally from Institute general and administrative funds, with no chargeback for services provided. Most clients were not heavily involved in the development of new applications. Often, they spent little time with analysts developing specifications, and, consequently, those applications did not meet their business needs. Partially because they did not pay for the services provided, many clients felt they did not have a strong stake in a new application's success.

For many years, the central application support group has included a team of full-time, professional technical writers (currently numbering six, plus a manager). In the past, clients had little input into the documentation process. Most of the manuals resulted from interactions between the writer and the application programmers. The level of contact and cooperation between the writer and the client usually mirrored that between the programmer or analyst and the client.

In this environment, the degree of success of a new application project was usually a factor of the individuals involved (on both the service provider and client sides), rather than as the systematic result of the processes, standards, and tools used. Results were mixed, with some projects succeeding and some failing. These mixed results provided much of the impetus toward implementing some of the changes described earlier.

Documentation in a Distributed Environment

In a distributed environment, application development is spread among our own development arena, using an application development methodology (Productivity Plus, licensed from the DMR Group Inc.) and development resources allocated to business units, which include outside applications development contractors, internal programming teams that may or may not adhere to a development methodology, and commercial packages (with or without vendor support and documentation).

Documentation takes on new roles under these varying conditions. It affects development in an ordered sense by requiring use of system specs and forcing their early refinement. It may be a vehicle to connect software bridges to packages. The writer works as a client advocate in the design of screens and usability testing for user documentation. ASD advocates that writers be included in the overall project plan and viewed as part of the development team, not adjunct to it. At MIT, the documentation team is frequently the only ASD team the client sees since he or she may be one of the business units using application development resources outside ASD.

Productivity Plus has brought home the importance of thinking before throwing those shrinking dollars into the first hole that looks attractive. It prescribes a route

for developing and documenting an application. In fact, deliverables like the preliminary analysis reports that detail the business requirements and proposed solutions become a "gateway" to obtaining project funding through the Administrative Computing Steering Committee at the Institute. The purpose is always to balance time and costs with the most functionality possible. In a time of careful money the question of the usefulness of documentation is raised often. In a chargeback organization the reasons for including it must be especially viable.

The methodology supports our notion that documentation adds substantial usability and ease of maintenance to an application. Seeing those values is easy if you live with the notion all the time. Explaining them to clients who are juggling development and operating resources is not so easy. Typically we hear that documentation is too expensive, there isn't enough time to do it, the client has the specs (well, we've SEEN those specs), and our all-time favorite, no one reads it. Given the complaints about documentation in magazine articles on software ratings, we suspect more than a few people sneak a glance at it now and again.

Instead of arguing about the issues, we try to get people to look at documentation with a "longer" view — as a snapshot or record, as an explicit interpretation of decisions about navigation, module relationships, functionality. Documentation is frequently used as a training vehicle and for developing testing protocols during maintenance programming. A full documentation set records the procedures and responsibilities of multiple constituencies — the users, the system manager, the programmers, in black and white.

Working with a Contractual Net

With this grounding, let's talk about structuring the documentation process to get real value. For one thing, we work with a couple of different kinds of contracts. Contracts do several things. They support the notion of individual accountability, and they legitimize an activity that often suffers from the skepticism of nonbelievers. The scheduling aspects prevent projects from becoming sinkholes.

Documentation Services' first layer is a Service Level Agreement or SLA. That's the level at which the project dollars and duration are worked out between offices, and people on both sides are committed to the project. The next level is a project plan which is largely constructed by the assigned writer with the assistance of the client contacts.

It is within this phase that the real hammering out of a documentation effort takes place. The writer takes any background information available — we hope a business requirements analysis or request for proposal, at least — and determines the level, scope, and preliminary content of a project. Meeting with the clients, he or she works out the objectives, content, schedules, testing, reviews, and production methods. This joint effort becomes the partnership that results in a better document. The project plan is the critical road map for a documentation project. Its schedule mirrors the development schedule, since the application development methodology rules state that we must deliver a system *with* its documentation. Signoff by all involved people is required before writing begins.

Project plans and Service Level Agreements are adjusted for the strange and wonderful things that can happen during the course of any project, particularly lengthy ones. Their iterations form part of the project record we describe below.

At the end of a project cycle we do two things. We ask clients to sign task acceptances as a way of formally turning over the documentation and signalling the end of our development involvement. We also ask the writer responsible for the project to complete a project summary. These summaries are designed to record all the phases of a project, the problems or variances, the normal processes, the places where we tried something new or used a different metric, the status reports and communications vehicles across teams, etc. This record is critical to planning similar projects and looking for change and trends in the documentation process.

In a dollar-conscious culture, projects summaries and project accounting mechanisms provide benefits to the client and to ASD. Used with our other project records, we can track real project hours and bill for real activities; we also can look for where we (clients and ASD) may need to refine a phase or change the way we perform an activity. However, we have noticed that this continuous monitoring can contribute to the vestigial paranoia that "pre-accounting era" staff members bring to projects. The upside is that we have discovered that this tidying up has the effect of bringing closure to the projects, a real plus for people working on multiple projects. They are then free to ramp up to devote the same energy level to the next project going into critical phases.

The team approach with development, the partnership with clients, and the ability to assume virtually total control over a documentation project means that the writers must be mature professionals who are capable of planning, creating working relationships, and communicating with colleagues, clients, and managers. They know their capabilities and rely on their own team to help increase their application and documentation knowledge bases. Our staff does not have entry-level writers. The writing and basic design skills of our writers are solid. Their technical training is as current as we can make it.

The writer as part of the development team must be a client advocate — transferring what he or she knows about the client and the needs of the office to the development effort. Documentation people often know the users better than anyone else. A writer also must get development team buy-in to the documentation process which is sometimes perceived as a burden on the technical folks. We try to make that process as painless as possible. The real professionalism comes in the tangible pieces of human factors engineering — screen design and logical procedures. Writers also participate in the testing of an application. As client advocates they are able to look at the application with the client's eye early on.

As with the case in most changing environments, we spend a chunk of our time educating our clients to "do the right thing". Engendering trust and assuring the client that they will benefit from the process we propose is ongoing — even with people who have worked with us before. We must remain mindful of their concerns and yet focussed on what we know is the "right" way to provide documentation that will last that client through the long haul.

Working with Clients

Once the SLA has been signed and the project plan has been written and accepted, the focus shifts from management to the day-to-day operation of the documentation project. At this level, the ASD technical writer works with the programming or administrative staff in the client office. Several aspects of this relationship bear on the value-added nature of the documentation produced. These aspects are:

- expectations that the client brings to the project
- expectations that the writer brings to the project
- client education
- project team participation
- advocacy
- quality assurance
- efficiency of operations

The first two aspects focus on the expectations at the beginning of the project, while the other five aspects concern how the writer works to deliver the manual that has been contracted for. We examine these in closer detail in this section.

- **Client expectations.** The client staff working on the project have expectations that have been passed on from the client manager or administrator who signed the SLA and project plan. Client staff expect that:
  - The writer will deliver what was contracted for. For example, if the project plan describes a 80–100 page manual for data entry operators, then at the end of the project this is what the writer will deliver.
  - Staff in the client office are involved throughout the life of the project. Their primary role is to provide information to the writer; other special roles (such as reviewer or documentation tester) are defined in the project plan. The writer doesn't disappear after the plan is signed and then magically reappear to deliver a finished manual three months later. A writer writes **about** an application or a system, but because the writer writes **for** people he or she must work **with** people.
  - The writer will communicate with the client staff during the project, since the project plan specifies weekly meetings and monthly status reports. This communication ensures a manual based on the client office's needs.

- **Writer expectations.** The writer also has expectations about the project. Some of these expectations were formed during the writing of the project plan, while others come from experience with previous projects. The writer expects that:
  - The client will be responsive. Because the client's responsibilities are defined in the SLA and the project plan, the client manager is able to plan to make time, resources, and reviewers available — the client office has money invested in the project and will want to be part of the process to ensure that the final product is good.
  - He or she will know what the project goals are, since these are clearly defined before writing begins. For example, if the project plan describes a 40–50 page manual for a billing module, the writer won't be surprised part way through the project with a request to document an accounts payable module as part of the same manual.

- **Client education.** During a project, a writer works to educate staff members in the client office about the content and quality of their documentation. This educational activity is ongoing — it doesn't consist of a five-minute pep talk at the beginning of the project. Some areas covered are:

- The writer periodically may have to justify full documentation for an application, keeping in mind both the immediate and the long-term readers of a manual. For example, a manager may say, "Keep the manual short, you can skip the stuff about logging on, my staff already know about that because I've trained them well." (Sometimes the manager thinks that a shorter manual will take less time and, therefore, less money.) In reply, the writer can acknowledge that, while the staff are well trained, a new staff member may need to substitute on short notice, or that sometimes even well-trained staff need to review procedures. The writer also might point out that the three or four pages of explanation will add little to the total writing time.
- The writer may have to explain having complete documentation as a backup in case of a "critical incident" — for example, the manager being hit by a bus while crossing the street at lunch, or the only data entry operator knowledgeable about the security system winning the lottery one day and quitting the next.
- The writer may need to remind a client to provide all the information needed for a particular procedure. For example, the writer may explain that it is important to provide a table of numerical codes for a two-character state field on a screen. If this information is omitted from the instructions, the data entry operator may use the zip code letters instead. While this error can be flagged for correction easily with an error message, it saves time and keystrokes to provide the information in the manual.
- The writer is responsible for managing the documentation project. If necessary, the writer will remind client staff about their responsibilities and the deadlines of the project.

Client education is an ongoing effort that affects all levels of interaction between the central application development group and clients. Figure 2 illustrates how this effort can be seen as a triangle.

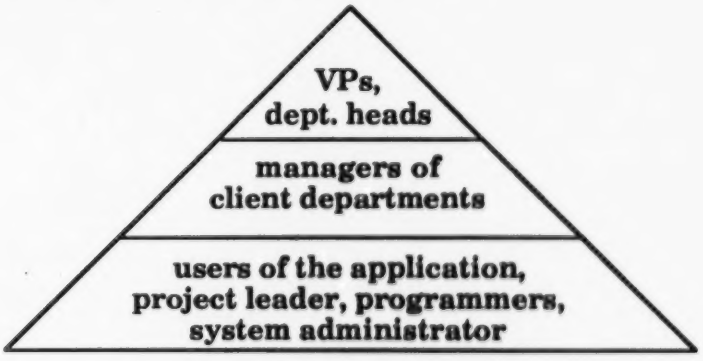


Figure 2. Levels of client education.

Client education occurs on a face-to-face basis, customized for each interaction.

- At the top level, involving a small number of people, the Director works with his peers, the vice presidents and department heads, to educate them about the importance of documentation in their long-term planning and budgeting for application development. This educational effort is general in nature and may not be focused on a specific project.

- At the middle level, the manager of the writer group works with managers in client departments to negotiate SLAs and project plans, and in the process educating them about the need for quality documentation.
- The writer on a specific project works at the bottom level of the triangle to educate the project leader, application users, programmers, and/or system administrator as the writing proceeds. While this effort may involve a larger number of people, it is also the most focused, since it may involve the importance of including a diagram or a table of field values or a short chapter on logging on. In this case, the writer works to demonstrate why the documentation is important to these day-to-day users of the application.

Client education is iterative at all levels of the triangle, in the same way that we must be always emphasizing quality information systems

- **Project team participation.** Having the writer integrated into the development team is a trend noted in both project management and technical writing journals. In addition, the application development methodology used at ASD mandates client involvement during project development. The writing staff has an important role in that interaction.
  - The writer understands the application better if he or she is involved from the beginning. This understanding makes writing the manual easier and quicker, since the writer has a larger context to explain the application to the reader and does not need to learn the application before writing about it.
  - The writer brings another viewpoint to the day-to-day programming effort. Frequently the writer may spot gaps or weaknesses in an application. For example, while testing a data entry screen for an investment management system, a writer may notice that the system accepts 1992 in a field for the current year. Since this field is used to compile the value of investments owned in a certain year, the mistake can lead to an error in the dollar totals. The programmer may not have realized that a program check is needed to guard against typing errors such as "1992" for "1991".

As this example points out, the writer is in a fragile place here, with a foot in both camps — the development team and the client office. This highlights another aspect of the writer's role — being an advocate for the system user.

- **User advocacy.** Even though the writer is contracted to produce documentation, the writer's ultimate responsibility is to the system user. The writer can ensure that both the documentation and the application interface (screens, reports) meet the users' needs. As an "outsider" (non-programmer) on the development team, the writer can advocate for a better developed system. Three examples can demonstrate this position.
  - A programmer, with an "insider's viewpoint", may use the mnemonic command "P" for "purge", a command frequently used with mainframe computer systems. However, in a Macintosh-based application, "P" almost always means "print ". With an "outsider's viewpoint" (that of the user), the writer can spot this problem and can explain to the programmer how the user expects a consistent use of commands across a system. (The programmer may already know this, and merely needs another pair of eyes to spot the mistake.)

- The writer understands how a user may approach a system. People who use several applications during the course of a day may enter dates in different ways for each application; non-English speaking staff may not know what date format to use. The writer can insist on having on-screen instructions or on-line help for date fields to demonstrate or explain the correct format.
- The writer can reword an error message such as "code 914 error; fatal" into something less drastic and more helpful, thus helping the reader to more quickly understand and correct an error.

- **Quality assurance.** Three aspects of quality assurance are important here.
  - The writer ensures that the manual meets the quality assurance standards used by the writing group. These standards help to prevent omissions in the manual's structure as well as to ensure internal consistency.
  - The manual also has a complete grammar and format edit.
  - In addition, the manual must meet the project goals as defined in the SLA and project plan at the beginning of the project.

- **Operating an efficient writing group.** The final aspect of working with the client focuses on the internal management of the documentation group. An efficient writing group can be achieved by several of the following techniques.
  - Using word processing and layout software efficiently frees writers to devote more time to writing.
  - Developing templates provides for quick development of documents and results in a consistent format and structure for work produced by the group ("corporate look"). For example, a writer can produce a title page with the group's logo and complicated format in only a minute or two by filling in the blanks on a template.
  - Writers share their experience on projects and solutions with each other. For example, once a writer develops a graphic showing the keyboard of a popular microcomputer, the illustration can be used in several manuals.
  - Senior writers and an editor guide large projects and help troubleshoot problem writing areas. Thus, a writer in the documentation group does not work alone or unsupported, even most of the working time is spent with the project team staff.

Summary: Benefits of Good Documentation

The payoffs of quality documentation — the value added aspect of application development — are explained in the list below.

- **Professional feeling.** If the manual communicates by its look and writing that an application is easy and direct to use, the users will feel reassured about using a new application. A quality product with quality documentation communications to users that they are an important part of the organization. Staff may experience less frustration using an application and may actually work more efficiently; they also will feel better about their jobs.

- **Better applications.** Better in two ways: **for the user**, since the writer is a client advocate bringing human factors training and experience to the development

team, and **for the institution**, since studies show that well-documented applications need less staff for training and support after implementation.

- **Knowledgeable staff who can use the system better.** Full documentation for a system can be used for training when the application is introduced and for ensuring continuity of operations when new staff are hired. The background information and procedures needed to run an application are recorded in the manual.

- **More efficient systems.** Thorough documentation saves time by providing information when and where it is needed, thus reducing the number of errors made (and consequently reducing the number of keystrokes).

- **Lower maintenance costs.** Technical documentation can provide both the context and details for programmers who need access to information on all aspects of an application.

- **Marketing**, indirectly. Good products (well-developed systems with quality documentation) enhance your department's reputation.

With higher education budgets become tighter, quality documentation is increasingly important in application development, as information systems departments search for ways to more efficiently and effectively deliver their services. MIT has found that thorough manuals and other documents produced by a professional writing group are critical to the success of applications developed by its Administrative Systems Development group. Quality documentation has immediate payoffs — by improving the effectiveness and usability of newly implemented applications — as well as long-term benefits — by providing technical documentation for maintenance and ensuring continuity of operations in case of staff turnover or emergency situations.

ISSUES IN THE DEVELOPMENT OF A CAMPUS COMPUTING AND INFORMATION POLICY

Timothy J. Foley
Associate Director Computing Center
Lehigh University
Bethlehem, Pennsylvania

ABSTRACT

The growth and expansion of information technologies on campuses across the country has caused many universities to begin to develop (or modify existing) information policies. Many schools have begun to implement campus-wide information systems which are used by the majority of people on their campuses. Questions concerning moral, ethical, and legal obligations have arisen, which in the past have been overlooked or not even considered. Lehigh having implemented a campus-wide information system which is used by over 95% of the campus, has had to develop an Information Policy to address the growing campus concerns relating to the appropriateness of publicly available electronic information.

Lehigh's Information System allows individuals to post information without any filtering to both on-campus and off-campus messaging systems. While these facilities are very useful, they have raised serious concerns relating to system resource management, possible legal liabilities concerning the nature of the information, and also the placement of materials that are obscene and offensive. The following issues relating to the development of Lehigh's Information Policy are discussed: possible legal liabilities, censorship, resource management, information ownership, user responsibilities, and the approval chain.

INTRODUCTION

Between 1985 and 1986, Lehigh distributed microcomputers to its entire faculty and placed hundreds of microcomputers at its public sites. Connectivity to Lehigh's computer systems was provided through a digital PBX with over 8000 data connections. During this time, Lehigh also decided that one real value of all this connectivity would be to provide information resources to the entire community. A project was developed in the spring of 1986 to provide information resources to the entire Lehigh community. The on-line information system would serve as a centralized communication facility for the campus. Development work on the system was begun in May of 1986 with availability for the entire campus in January of 1987. This system, called LUNA (Lehigh University Network Applications), provided the following services: centralized electronic mail, bulletin board and conferencing facilities, access to external networks, on-line forms processing, access to high quality print services, and on-line survey facilities. The system has been highly successful [1]. Accounts on the system have grown from 200 in January of 1987 to over 6700 individual users in March of 1990 (see Figure 1). It should be noted, that users open their own accounts on the information system by running a program. This program also provides an electronic agreement to our information policy.

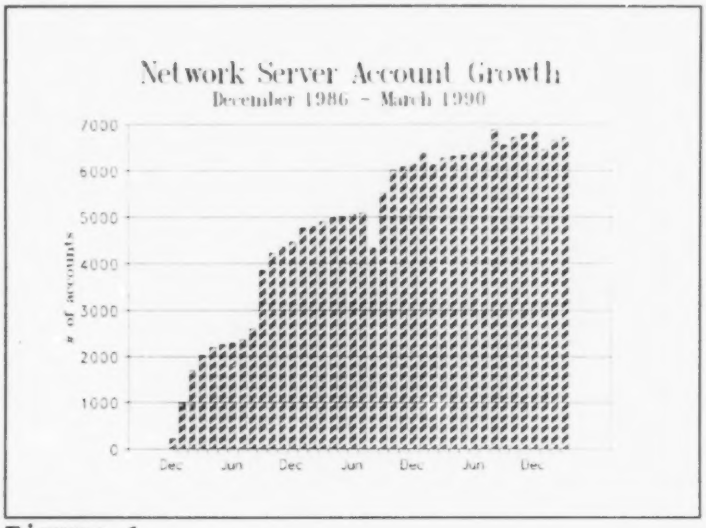


Figure 1

INFORMATION MANAGEMENT

The function of information management is distributed throughout the campus to the individuals, groups or departments responsible for the information. Information posted on the system for general access is monitored by the person responsible for the specific information. This person must have the approval of a faculty member, department head, or group advisor before being allowed to post information. This method of information management has resulted in the establishment of over 300 Information topics over the last four years. For example,

- The Research Program Development Office maintains a bulletin board of research funding opportunities.

- The Student Affairs Office utilizes the on-line survey facility to get feedback on the quality of education at Lehigh.

- The faculty software committee participates in a conference on software funding requests.

- The Computing Center maintains electronic libraries of public domain and site-licensed microcomputer software.

- The Human Resource Office maintains a listing of all available jobs on campus.

- The Library maintains on-line forms for interlibrary loans, Media Center request, and bibliographic search and reference questions.

Figure 2 shows some of the more popular topics and the number of times they were accessed over a one month period. As can be seen, the most popular topic on campus is items for sale. This topic has the most general appeal. The second most used topic is file transfer. Its popularity is due, in part, to the large amount of public domain and site license software available for downloading. It should be noted, that other items such as interlibrary loans which did not make the list had over 100 requests processed electronically per week.

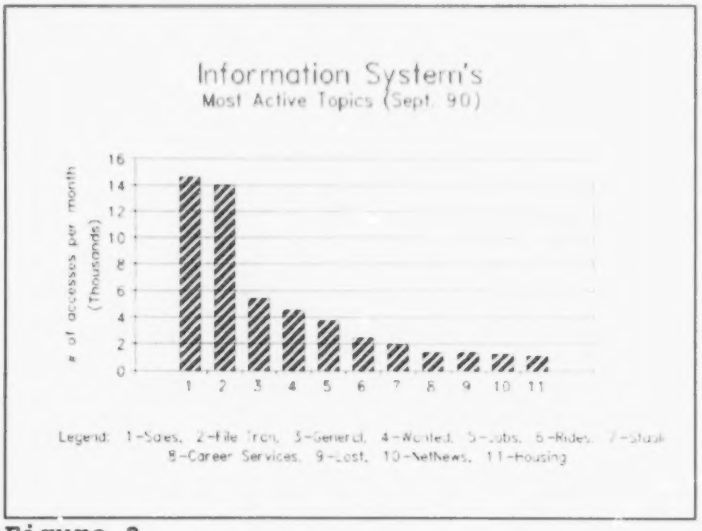


Figure 2

Initially, very restrictive controls were placed on an individual's ability to post publicly available information on the system. These controls have been relaxed to allow the instant posting of messages to conference and bulletin board areas. After a series of instances involving obscene, abusive, and offensive postings, the Computing Center realized that its current computer policies did not fully address many areas of abuse that were occurring on the information system. One student, for example, posted a message describing techniques for killing cats under our LITFORUM conference which was sponsored by an English professor. Lehigh's president then received a call from a local animal rights group asking that the message be removed. Another example, was the Human Diversity conference which discussed issues of homosexuality. After some very abusive comments to the conference, the Computing Center received a call from the Dean of Students enquiring about the faculty member responsible for the conference. Strange

BEST COPY AVAILABLE

as it may seem, the chaplain was the faculty member responsible for the conference.

Due to the large user base, the Computing Center felt that any policy decision regarding what was and was not appropriate on the information system should be based on a faculty, student, and staff recommendation rather than have users think that the Computing Center had arbitrarily decided what information should and should not be posted.

Once Lehigh decided to make the information from Usenet publicly available, the off-campus materials being posted on its system became an issue. The topics on Usenet range from discussions on sexual bondage (hot sex) to cold fusion. Control of the postings in individual topic areas was virtually impossible due to the magnitude of the information received, about 500 megabytes per month. Quotes such as:

> "The age of innocence is gone. Running a bulletin board means taking on certain legal and moral obligations." Jonathan Wallace a New York based attorney specializing in technology law. [2]
>
> "Running a BBS is becoming a business. And with that maturity is going to come a lot of potential legal liability." Paul Bernstein a Chicago attorney. [2]
>
> "One could see the headlines now X University found guilty of providing X-rated materials to minors" (Usenet message posted by a 16 year old attending Rutgers).

made the Computing Center more aware of the possible legal liabilities that the University might face in regards to information posted on their computing systems.

LEGAL LIABILITIES

Is the university responsible for publicly available information placed on its computer systems? Wallace and Morrison state that Information System operators should take "reasonable" steps to discover and remove any types of illegal material or libelous information that have been placed on an Information System [3]. The following are examples of illegal materials which may lead to a lawsuit or criminal charges: (1) pirated software, (2) credit card numbers, (3) "Trojan Horse" programs, (4) pornographic materials, (5) trade secrets. Knowing that the actual monitoring of the information on the system would be unmanageable by one group, the Computing Center has made each bulletin or conference coordinator sign an authorization form in which they agree to following the guidelines of our Information Policy.

The consequences of having illegal or "alleged illegal" material on your information system can be seen in the March 1, 1990, seizure by the Secret Service of 40 computers and 23,000 diskettes from Steve Jackson Games, an Austin Texas manufacturer who had a game that was described as a handbook for computer crime [4]. The Electronic Frontier Foundation (EFF), which was established by the Lotus Development Corporation founders Mitch Kapor and John

Barlow is trying to get the government to fully disclose all the facts of the seizure. The foundation was establish to address the social and legal issues associated with computer communication and information dissemination [5].

The Information Policy should also inform users of their legal liabilities. Many users are unaware of the serious nature and possible consequences of their actions and should be made aware of both federal and state laws involving computer abuse. An Information Policy should give examples of laws and penalties that can be incurred. For example Lehigh's Information Policy includes the following statement:

> Under Pennsylvania law, it is a felony punishable by a fine of up to $15,000 and imprisonment up to seven years for any person to access, alter or damage any computer system, network, software or database, or any part thereof, with the intent to interrupt the normal functioning of an organization (18 Pa.C.S. 3933(a)(1)). Knowingly and without authorization disclosing a password to a computer system, network, etc. is a misdemeanor punishable by a fine of up to $10,000 and imprisonment of up to five years, as is intentional and unauthorized access to a computer, interference with the operation of a computer or network, or alteration of computer software (18 PA.C.S. 3933(a)(2) and (3)).

CENSORSHIP

Does the university have a right to "censor" information which is posted on its computing systems? Should the university set standards for topics to be discussed or language to be used in computer communications? Lehigh decided that the answer to both of these questions was yes, when they applied to any publicly available information. An analogy can be made to the publisher of a magazine that shapes the content of its articles based on certain standards. Information posted on our computing systems that is publicly available to the entire Lehigh community would have to follow the guidelines posted in our Information Policy. An underground electronic press has sprung up as a result of the private conferencing facility that was made available to our users. Private messages and conferences are not subject to our information policy unless the messages infringe on another person's rights or are clearly illegal. Some examples are: the sending of abusive or obscene mail or the private conference that gave step-by-step instructions on building an HBO decoder. In general, the Computing Center feels that private messages and conferences are the responsibility of the individuals involved and does not monitor private mail or private conferences.

INFORMATION OWNERSHIP

Text files, messages, and programs placed on our information system are regarded as the property of the sender. Users are advised that they must abide by all copyright laws with regards to programs and text files. For example, the practice of excerpting magazine or newspaper articles and placing them on an information system is technically a violation of copyright laws and is not allowed.

The Computing Center regards all private messages and files as belonging to each individual user. The Electronic Communications Privacy Act of 1986 (ECPA) makes the disclosure of any private messages to a third party a federal misdemeanor. The Electronic Mail Association has recently issued a white paper recommending that companies adopt a formal policy regarding the privacy policies of all media communications [6]. Lehigh's Information Policy does allow for the monitoring of individual files when there is a clear threat to system security by an individual, but not without prior approval by the Director of the Computing Center. It is important for users to understand that private communications will not be monitored without extenuating circumstances.

USER RESPONSIBILITIES

Part of the development of any information policy is the mechanism that needs to be in place to inform users of their responsibilities to abide by these policies. As stated previously, it is important for users to be aware of the seriousness of computer abuse and information regarding the laws associated with computer abuse. These laws should be clearly stated in an information policy. At Lehigh, our Computing and Information Policy statement is agreed to by the user when they first open an account which accesses our Information System. The policy is also contained in the Student Handbook, "Intro to LUCC", and on authorization forms for other computers. Conference and bulletin board moderators also sign a form agreeing to regularly monitor their topic areas to make sure that they are in compliance with the Computing and Information Policy.

RESOURCE MANAGEMENT

Resource management covers many areas which must be addressed in a policy statement. Users must be informed of the consequences of sending unsolicited junk mail such as chain letters. They also must be informed of the consequences of computer hacking and unwarranted use of systems resources such as excessive printing or creating unnecessary network traffic.

As an information system gains in popularity as a tool for campus-wide communications, users begin to make special requests for mass mailings, login messages, or even special placement within the information system. A policy must be developed and the information system manager must cope with the political aspects of information flow management where one must try to minimize "junk mail" while maintaining a good working relationship with university constituents who feel that the information they want posted is very important to everyone. With over 5000 logins per day, the Computing Center has tried to follow the policy of only posting login messages or sending mass mailings that are relevant to the user community at large (see Figure 3). This policy does get modified at times, however, depending on who is asking for the login request or mass mailing. In these cases, the Computing Center informs the user community of the sender of the message so complaints about "junk mail" can be directed to the requestor and not to the Computing Center. Another request that is frequently made is for placement on the

main Information and Services menu. Our policy on this is to keep all departments off the main menu except for the Research Department and the Library. These two departments along with the Computing Center were the first users of the Information and Services facility and provided the Center with useful application ideas, such as on-line forms and the overall bulletin board structure. They also helped the Center market the system by providing incentives such as research coffee mugs for accessing the research bulletin board and special documentation of the Library services provided on the information system. Requests for special placement have also been reduced by the implementation of an update facility which tells a user what topics have changed within any specified time frame.

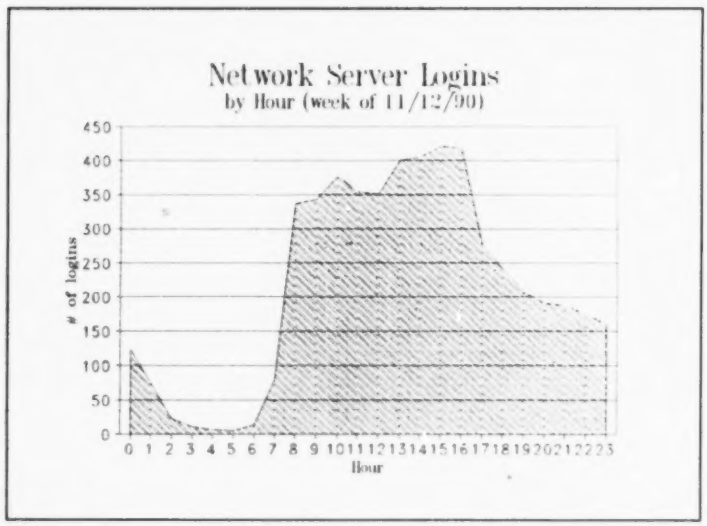


Figure 3

Another concern in resource management was the traffic created by a larger external information systems such as Usenet, which can create over 500 megabytes of information per month. The Computing Center initially withheld Usenet availability due to the large amount of traffic and the nature of some of the postings. The Computing Center's Advisory Committee recommended that the Center only make topic areas available that were directly related to the educational process. Other topics could be added, but they had to be requested by a faculty or staff member.

APPROVAL CHAIN

Following the proper approval chain is important in an university environment. Making sure that one's superiors are aware of the possible consequences and problems associated with running and maintaining an information system is critical. At Lehigh, the first step in the approval chain is our Computing Center Advisory Committee (CCAC), which is composed of faculty, staff, and students. Having the CCAC approve and shape the content of the information policy also lets users know that the policy was derived from their representatives rather than just being arbitrarily implemented by the Computing Center. Our policy statement was approved by the CCAC with a recommendation that it be reviewed by the University's legal representative. The Provost, however, felt that the policy statement only needed the CCAC's approval and that legal opinions were unnecessary.

In general, it is probably best to have the Information Policy approved at the highest level possible at your institution and also to have the document reviewed by the institution's attorneys to try to minimize any possible legal liabilities. Contacting the school's risk management department and internal auditor might also be useful concerning the content of the Information Policy.

LEHIGH'S CURRENT POLICY STATEMENT

Those who do not abide by the policies listed below should expect suspension of computer privileges and referral to the University Committee on Discipline.

Offenders may also be subject to criminal prosecution under federal or state law, and should expect the Computing Center to pursue such action. As an example, under Pennsylvania law, it is a felony punishable by a fine of up to $15,000 and imprisonment up to seven years for any person to access, alter or damage any computer system, network, software or database, or any part thereof, with the intent to interrupt the normal functioning of an organization (18 Pa.C.S. 3933(a)(1)). Knowingly and without authorization disclosing a password to a computer system, network, etc. is a misdemeanor punishable by a fine of up to $10,000 and imprisonment of up to five years, as is intentional and unauthorized access to a computer, interference with the operation of a computer or network, or alteration of computer software (18 PA.C.S. 3933(a)(2) and (3).

The Computing Center should be notified about violations of computer laws and policies, as well as about potential loopholes in the security of its computer systems and networks. The user community is expected to cooperate with the Computing Center in its operation of computer systems and networks as well as in the investigation of misuse or abuse. Should the security of a computer system be threatened, user files may be examined under the direction of the Computing Center Director.

The Center's computer resources and facilities are solely for the use of Lehigh (registered) students, faculty and staff, with the exception of those paying to use mainframe applications which are otherwise unavailable locally.

POLICIES

The Computing Center's policies include but are not limited to the list below.

1) You must not use a computer ID that was not assigned by LUCC to you, unless multiple access has been authorized for the ID by LUCC. You may not try in any way to obtain a password for another's computer ID. You may not attempt to disguise the identity of the account or machine you are using.

2) You must not use the Computing Center's network resources to gain unauthorized access to remote computers.

3) You must not deliberately perform an act which will seriously impact the operation of computers, terminals, peripherals, or networks. This includes but is not limited to tampering with the components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer.

4) You must not attempt to modify in any way a program diskette which the Computing Center supplies for any type of use at its sites.

5) You must not run or install on any of the Center's computer systems, or give to another, a program which could result in the eventual damage to a file or computer system and/or the reproduction of itself. This is directed towards but not limited to the classes of programs known as computer viruses, Trojan horses, and worms.

6) You must not attempt to circumvent data protection schemes or uncover security loopholes.

7) You must abide by the terms of all software licensing agreements and copyright laws.

8) You must not deliberately perform acts which are wasteful of computing resources. These acts include but are not limited to sending mass mailings or chain letters, obtaining unnecessary output, creating unnecessary multiple jobs or processes, or creating unnecessary network traffic.

9) The following types of information or software cannot be placed on any system on- or off-campus:

* That which infringes upon the rights of another person.
* That which is abusive, profane, or sexually offensive to the average person.
* That which consists of information which may injure someone else and/or lead to a lawsuit or criminal charges. Examples of these are: pirated software, destructive software, pornographic materials, or libelous statements.
* That which consists of any advertisements for commercial enterprises.

10) You must not harass others by sending annoying, threatening, libelous, or sexually, racially or religiously offensive messages.

11) You must not attempt to monitor another user's data communications, nor may you read, copy, change or delete another user's files or software, without permission of the owner.

12) You must not use any of the Center's microcomputers, workstations or networks for other than a Lehigh University course, research project or departmental activity. These resources

must not be used for personal financial gain unless in support of a Lehigh University research or departmental project.

13) You must not use a computer account for work not specifically authorized for that account. A University-funded account may not be used by its requestor for personal financial gain.

14) You must not play games using any of the Center's computers or networks, unless for instructional purposes as specifically assigned by a professor.

The above policies supplement the University Code of Conduct, which covers such acts as theft of computer services (including copyrighted computer programs), theft or mutilation of Lehigh property such as equipment, and the unacknowledged or unauthorized appropriation of another's computer program, or the results of that program, in whole or in part, for a computer-related exercise or assignment.

Software developers should refer to the "Procedure on Software Disclosure and Development" regarding title rights.

REFERENCES

1. T. Foley, "Managing Campus-wide Information Systems: Issues and Problems" Proc. of ACM SIGUCCS User Services Conference XVI, p. 169-174, 1989.

2. B. Meeks, "As BBSes Mature, Liability Becomes and Issue" Infoworld, Volume 12 Issue 4, Jan. 22, 1990, p. 14-15

3. J. Wallace & R. Morrison, Syslaw (LLM Press, NY, 1988)

4. S. Mace, "Kapor and Wozniak Establish Electronic Policy Foundation" Infoworld, Volume 12 Issue 29, July 16, 1990, p. 6

5. Electronic Frontier Foundation, One Cambridge Center, Suite 300, Cambridge MA 02142

6. B. Brown, "EMA urges users to adopt policy on E-mail privacy" Network World, Volume 7, Number 44, Oct. 29, 1990, p. 2

THE RIGHT MIX: ATMs AND VRUs IN THE ADD/DROP PROCESS

John J. Springfield
Boston College
Chestnut Hill
Massachusetts

The add/drop process usually occurs during a concentrated (and often frantic) period of time. If the time period or methods of access could be expanded, the add/drop process would be less of a burden to students and staff. As part of "Project Glasnost" at Boston College, we have combined VRUs (Voice Response Units) with cashless ATMs (Automated Teller Machines) to allow students to change courses and list their class schedules easily.

Voice response units allow students to phone in their course changes starting six weeks before the beginning of the semester. To list their courses, students may listen to the list of their courses on the phone. However, most students still want a paper copy of their schedule. Students then turn to our cashless ATMs (with 80-column printers) to print out their full course schedules. Both VRUs and ATM's require a Personal Identification Number.

By combining the two technologies with traditional "in person" service, student access is enhanced and the load is distributed over time and devices.

Project Glasnost - Opening up Access

Several years ago Boston College started "Project Glasnost", a long-range project to open up the mainframe computer to the the university community, especially the students. In February 1989 we became the first university to allow students to access their courses, grades, schedules, student loans, student accounts, and other information via a cashless ATM (Automated Teller Machine). The overwhelming success of the ATM (40,000 inquiries per year) encouraged us to find other ways for students to become active participants in the management of their records.

We Hate Standing in Line

When we asked students and administrators what the most important problem was in servicing students, the cry was almost universal: "Can you please do something to eliminate waiting in long lines?" The natural bottlenecks created by registration and add/drop drew the biggest complaints.

Bottlenecks were due to these factors:

- All 8000 undergraduates had to go through registration at one central site. Many students returned during add/drop period to change courses.
- Registration and subsequent add/drop periods were concentrated in a short period of time.
- Even with assigned registration times, students arrived early to make sure they didn't miss their "slot".
- Since add/drop period had no assigned times, students lined up early in the morning hoping to into a course.

Possible Solutions

No all problems can be solved by a high-tech answer. Some may only require a low-tech solution. Long lines are created because more people arrive at a destination than there are people to service them. A low-tech answer is to simply extend the time period. This will work with registration because people can be notified to appear at a designated time. But add/drop is a basic free-for-all. Students cannot be assigned to times because the process is dynamic. A course that is closed today may be open tomorrow. Students want to be able to try several times to get the courses they want.

Add/drop seems to require a high-tech solution. If a staff person could be replaced by a VRU or ATM, maybe the demand could be satisfied. Boston College students have been using cashless ATMs to get a printout of their courses, schedules, grades, and financial information. Perhaps we could use the ATMs for adding and dropping courses? At first it seems natural. The security is already builtin, all courses have unique index numbers, and the students could get an immediate course printout. However, now we have simply moved the lines from the registrar to the ATMs. Not only would students be waiting in line again to add/drop, but other students who only want to look up financial information would be stuck in the same lines. It was decided that the ATMs would continue to function to dispense information, not update it.

However, VRUs seemed more promising. Instead of servicing one student at a time, one VRU could handle many students simultaneously. If demand exceeded one VRU, they could be "chained" together. The students would call one number, and the phone system could "hunt" for the next available VRU line. Now the limiting factor was the number of incoming lines to the university that could be dedicated to the VRUs. The main drawback to voice technology is that is not visual. Things have to explained linearly, not spacially. And of course, students could not get an instant printout over the phone, but they could get one the next time they visited one of the campus ATMs.

Human Factors

In designing a new system we realized that not all students would or could take advantage of new technologies. Voice registration certainly helps the majority of students who have straight-forward course requirements. But some students will be required to have written permission from departments to take certain courses. Some students have "holds" on their registration that require visits to the registrar or student accounts offices. Some require special overrides that can only be resolved by visiting the registrar. And then others simply want to talk to a human being.

Interestingly, even students who are comfortable with phone registration still wanted a printout of their courses. It seems to be a needed reinforcement to "get it on paper".

It was decided that human factors dictated that a new system would include the following:

- Students would be allowed more that one method to register and add/drop courses: in-person and VRUs.
- To assure equal access, both systems would access and update the same mainframe files.
- Students wishing an immediate confirmation of their schedules could visit the ATMs on campus. Others would be sent a confirmation via a batch program.

Technical Factors

Of course wishing for an easy solution does not make it reality. Technical problems of resources had to first be solved. We had to look at the impact on the mainframe (CICS) as well as the increased phone traffic.

After some initial tests, we concluded that the CICS and the mainframe could easily handle the increased file accessing. However, we would need to limit the hours that students could call in order to do our usual batch processing at night. We were updating files real time. We didn't feel that the creation of redundant files was worth the extra convenience of calling 24 hours per day.

Our main concern centered around the increased phone traffic coming into the university. We had two VRUs: the IBM 9274 (12 incoming lines) and the IBM 9270 (4 incoming lines). We needed to make sure that the amount of calls coming into the university did not tie up all the lines. But we also needed to service the students so that we didn't cause "lines" waiting for the VRU lines to be free.

Technical considerations prompted the following set of restrictions:

- The VRU could be called between 8 a.m. and 7 p.m.
- The overall add/drop period would be extented to begin 6 weeks before the beginning of classes, immediately after advanced registration. By lengthening the period, we hoped to reduce the number of calls per hour.
- If more calls were received than the VRU could handle, a pre-recorded message would say to hang up and call back or come to the registrar's office. The recording was programmed into the phone system, and it could be changed at any time, independent of the VRU.

Security Factors

All access to the VRU and ATM required a PIN (Personal Identification Number) as well as the corresponding student ID number. The VRU required the entry of the student ID, while the ATM required the insertion of a student ID card with an encoded ID number.

Students were notified of their PIN when becoming a student. If they forget their PIN, they may go to a designated office and receive their PIN if they presented their picture ID card. The procedure is administered by the the MIS security administrator. Request for new PINs require a written request and a 1 day turn around

Acceptance of System

The VRU was tested on a small group of political science majors during August 1990. The response was enthusiatic from the students and the registrar.

In November of 1990 we started allowing all 8000 undergrads to register and add/drop via the phone (as well as in person). 3/4 of the students used the VRU, but many still required the services of a staff person.

Students were allowed to add/drop as soon as they had registered. During registration period, 100 students per hour were scheduled. The VRUs could accommodate approximately 125 calls per hour using 15 incoming lines. As can been seen on the following chart, many students called back to try to rearrange their schedules during the November 1990 registration period:

NUMBER OF TIMES STUDENTS CALLED	PERCENTAGE OF CALLS
1	59%
2	22%
3	8%
4	4%
5 or more	7%

As of this writing, add/drop period is still in progress. Since November registration period is over, it is hoped that the VRU traffic for add/drops will not exceed 125 per hour.

Future Enhancements

VRUs are clearly a step in the right direction. They allow better throughput than in-person add/drops. However, VRUs depend on a person understanding directions by hearing, not seeing. But this is a "visual" society. Most people use sight more than hearing to process information. Probably the best way to self-register and to add/drop is to use a terminal or personal computer with a modem. Computer screens allow the student to "paint" in the whole schedule at one time, instead of entering one at a time via the phone. Terminals can give more options to the students when a course or its corequisite is filled up. Unlike the phone, terminals are not time-sensitive: you can stay on the terminal as long as you like without seriously impacting another student.

In a test project we allowed about 300 student employees to register and add/drop via terminals in their offices. The overwhelming response was that this was even better than using the phone. Remember, these students were very familiar with the terminals. However, because most students are not familiar with the IBM keyboards (especially cursor keys), we realized that a "front-end" would have to be designed to facilitate terminal use for novices. The front end could be created on a MacIntosh to take advantage of the point-and-click technology.

But not all students have the same access to terminals or PCs as they do phones. We have to be concerned that we have a common playing field. So it seems that the future will bring three kinds of registration access: in person, phones, and terminals. As long as their is equal access, students should be able to make the choice that fits their circumstances.